BYOD with Security

Ulysses Moreira das Neves, and Flávio Luis de Mello

Abstract— The concern of companies to keep sensitive data protected from improper access and information leaking has grown a lot. The constant cases of industrial espionage and information leakage regarding companies are an evidence of the need to apply strict information security policies, improve data protection and allow an auditing track. With the evolution of technology, the usage of personal mobile devices increased in organizations (BYOD - Bring Your Own Device), which allows the employees to use their own mobile devices at work. This paper addresses the current challenges faced by IT companies and teams in protecting access to this kind of information, and what strategies are used to mitigate, to track leaks, and reduce the misuse of documents in the organization. Considering the scenario evaluated, a framework with good Information Security practices based on the ISO 27002:2005 and the practical controls of the Center of Internet Security (CIS) is proposed, associating good practices with the needs of BYOD's culture. The framework suggested in this paper reinforces the necessity for a standardization of the rules of information security in the process of adoption of BYOD's culture, following the life cycle of the user with his personal mobile device in the company.

Index Terms— BYOD, sensitive data, information security, security framework.

I. Introduction

THE theme of this work is the growth of the use of personal devices in corporate environments, the advantages and disadvantages that this practice has brought to companies and employees, and how the companies are dealing with the classification, storage and control of corporate data access with the adoption of BYOD technology. In this sense, the problem to be solved is to simplify the implementation and maintenance of BYOD's culture in the company through a framework focused on protecting data stored in the users' personal devices based on ISO 27002:2005 information security standards and CIS controls.

The technology's evolution has made it easier for end users to access mobile devices every year. This, in addition to the Internet's mobility, favors the emergence of BYOD's culture, where a collaborator uses his own device to access information that was previously accessible only from the computer located in the corporate offices. This movement has contributed to the reduction of costs and optimization, since users would already be familiar with their own devices. However, such circumstance has brought a great concern to companies and IT such as the necessity for protecting the corporate information stored on the user's device during the exercise of their activities. Today, companies rely on numerous tools to support mobile device control and information security standards that offer good practices in protecting this information, but these standards do not directly address the needs of companies involved with BYOD's culture, making it difficult to IT team to deal with planning, implementing and maintaining security in this data.

This work's aims to compile threats and difficulties concerning the protection of sensitive data and to present a framework focused on mobile devices, based on ISO 27002:2005 standards and CIS controls that address data protection strategies, in companies where BYOD is already reality. The paper discusses the concept of information security policies and how they can be applied in conjunction with the use of support tools to protect the company's confidential data. Once such security policies are shown, a framework is presented. It is divided in three cycles composed of good practices that can be used in the corporation to correct vulnerabilities of information security for BYOD.

The standards established by ISO 27002:2005 and in the CIS security controls provide theoretical establishment to propose a framework based on cycles, where it becomes possible to measure the company's maturity in mobile device safety, and also to support the identification and correction of possible identified failures. At the end, a case study is presented with three companies, evaluating information security vulnerabilities with BYOD based on the guidelines presented in this paper.

II. Related Work

ISO 27002:2005 defines the classification of information of extreme importance to guarantee the protection of information in the corporate environment. According to ISO 27002:2005, it is recommended to use an information classification system in conjunction with data categorization policies to determine to which category the information belongs and to define what kind of policies will be applied to ensure the protection of this information [5]. According to ISO 27002:2005, the classification of this information must be

Submitted for review on December 9th, 2018. This work was supported in part by Machine Intelligence and Computer Models Laboratory of Federal University of Rio de Janeiro (IM2C/Poli/UFRJ) under grant Poli 19.257 of Coppetec.

Ulysses Moreira das Neves is SystemAdmin at Fundação Getúlio Vargas, Brazil. (uneves.moreira@gmail.com).

Flávio Luis de Mello (D.Sc.) is associate professor at the Electronics and Computer Department from Polytechnic School at Federal University of Rio de Janeiro, Brazil (email: fmello@poli.ufrj.br).

updated periodically, and the protection policy of this data must be revised according to the rules defined in the organization. CIS states that it is important to the corporation understands the definition of sensitive information and the importance of the classification of access levels. Based on this classification, the impact to the business is analyzed when this information is accessed by unauthorized or leaked personnel [3]. The CIS reports that, after the information classification, the company must use logical and physical protection in the information security. Network segregation, firewalls access controls, and network access permissions can be used as protection.

Gajar et al. [4] address the emergence of BYOD's culture, the technologies that have fostered this emergence, benefits and challenges of this new modality of work. The authors of the article also discuss the threats, risks and strategies that can be followed to mitigate these issues in BYOD's environment. The article presents metrics and support controls to protect users' personal devices, and then it proposes an architecture of a mobile device management solution. As a conclusion, the authors suggest the creation of a model for treating threats in BYOD's universe and practical controls to apply the norms.

Zahadat et al. [5] talks about the emergence of BYOD, the evolution of devices and pioneering. Its approach is similar to this work, the authors cite most critical security flaws in BYOD's scenario, including: inconsistent security policies, shared media leaks, minimal management of mobile devices, company data that remain readable on devices and data leakage between applications. The article presents the concept of a framework based on cycles containing registration, provisioning, operation and removal, guiding organizations how to plan, identify, protect, detect, respond, retrieve and evaluate mobile devices.

Rivera et al. [6] talks about the emergence and benefits of BYOD but warns about security risks of stored information in personal mobile device and company embedded data. The authors address technologies that support BYOD, like desktop virtualization, network access control, device management, access control mechanisms, mobile application manager, threat control, antivirus for mobile devices and cloud computing management. The authors also compare the data protection controls with the technologies mentioned above. Such article influenced the collection of tools to support the IT team in the management and protection of BYOD corporation assets.

Alharthy e Shawkat [7] concerns with network protection measures where BYOD usage is allowed. It divides the research into data collection, analysis, network design, and security implementation for BYOD. The article includes studies on network usage through mobile devices, server infrastructure. It also includes suggestions for improvements in processes and information security's management regarding BYOD infrastructure.

Ali et al. [8] make threats analysis on the use of personal devices at companies. Based on the same concept of this work, the authors talk about safety requirements for BYOD, presenting good practices that help companies to mitigate risks brought by this scenario. The article divides BYOD's security model into personal device management, kernel modification, and VPN access modeling. With this division, an access to sensitive, restricted and unrestricted data architecture is proposed, each dealing with one or a combination of different technologies.

Peng et al. [9] talk about the importance of protecting mobile devices in a network. It presents a strategy to protect these devices through a network of secure infrastructure that run autonomous agents and, fulfilling a security requirement. It presents a solution where a device identified as some type of threat is immediately located and treated. The work presents an algorithm that joins mobile devices into groups and assigns them monitoring devices from other mobile groups, creating a set of protected devices and ensuring that everyone is checked and free of infections.

Armando et al. [10] focal point is the risks that BYOD brings to the business, as well as the research presented in this document. The authors identified that the market's MDM technologies do not works at environments that are more complex, and they developed a software for the company NATO Communications and Information Agency called BYODroid. This project is focused on developing an application for managing BYOD devices in environments that are too complex to be managed by MDM tools.

Lee et al. [11] reinforce the need to control users' personal mobile devices in a company. The authors explain the differences in authentication between MDM and MAM technologies from Android, IOS and Windows operating systems, suggesting good deployment practices when using these technologies. The authors also presented in detail the communication architecture of a device and the servers which manage and monitor the accesses and applications, reinforcing the control needs of these devices.

Lee et al. [12] propose a secure content pre-verification system available for BYOD devices. The work suggests that the solution should be managed by the government or some independent body, supporting application control and integrated with MDM software that automatically, and in real time, release or block applications for BYOD devices.

Bello et al. [13] present a research done among employees of three companies that use BYOD, raising risks, threats and challenges in the implantation and maintenance of this culture. At the end, the research presents a summary of data collected through the interviews and some technical solutions to mitigate the risks that were raised.

III. Framework BYOD with Security

IN in this section it is presented a framework called BYOD with Security that provide a guide to good information security practices for consumerization's culture adopted in companies, based on pre-defined problems.

The problems presented in this work were selected based on the risks of information leakage mapped throughout the current research, and on the guidelines of ISO 27002:2005 and CIS controls. Such problems are enumerated as follows:

- P1: Users in transit who need access to company's network to work on sensitive data using their personal devices.

- P2: Access security issues with the additive of data integrity issues.
- P3: Lost or stolen personal computer device without password or biometrical security to restrict access to confidential information.
- P4: A sensitive area employer or a strategic company manager hired by a competitor and who takes information to this new company.
- P5: Protect the original document to ensure the information's integrity and prevent other people from questioning the document's originality or content.
- P6: Users with personal devices without proper licensing from the manufacturer or with improperly unlocked functions.
- P7: Legal challenges regarding use of the mobile device remotely.
- P8: User's personal devices connecting to insecure networks, called hot spots, may have their devices compromised, affecting the company network by connecting it to the office infrastructure.
- P9: Communication between company's personal devices may suffer incompatibility problems due to the diversification of each user's models and operating systems, causing problems for IT management of these devices.
- P10: IT staff may have problems with obsolete operating systems that are no longer supported by the manufacturer, combined with the absence of user interest in upgrading it.

The policies proposed in this paper are based on the standard of information security techniques ISO 27002:2005 and on CIS information security controls with a focus on BYOD devices. The guidelines defined in this document should be considered as a starting point and can be adapted depending on the company or process needs.

In the present proposal, the process of using own devices is divided into three stages, namely: (1) commissioning in BYOD's culture, (2) monitoring and control of device usage and (3) discharge program. The flow of BYOD's program seeks to continuously improve information security practices based on the experiences gained during monitoring and control, as shown in Figure 3.1. The commissioning in BYOD's program is the stage where the user requests the entry of their personal device into the company network justifying the need for their professional activities. The monitoring and maintenance stage presents tools to support the control and maintenance of the safety of BYOD's devices described in the next paragraphs. BYOD's discharge program provides guidance on actions that must be taken to ensure the cancelation of all asset's accesses whenever exiting the program.

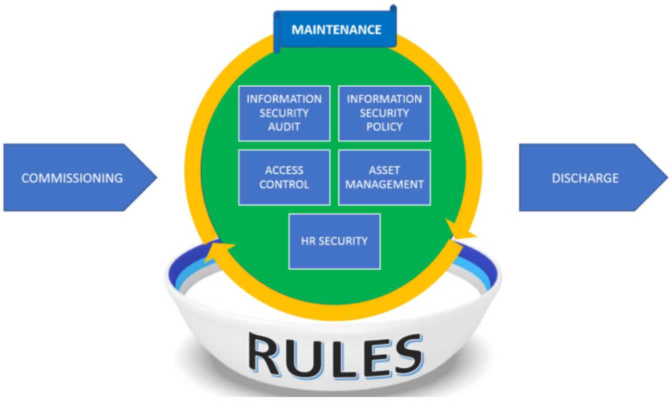


Figure 3.1. User life flow in BYOD's program.

For each new user, a procedure is defined to be followed and rules are enumerated so that to protect data effectively. The following subsections guide how to apply the process steps:

A. *Commissioning step in BYOD's program*

Considering that not all users have the need of caring company data, the user's BYOD security framework will adherent to company's business area demands and, if proven necessary, the company can apply the guidelines listed below:

- R1: The user should complete a certain amount of training hours on Information Security, understand the information classification flow, as well as device protection procedures, in transit or outside the company, and acknowledge the actions to be taken in in case of loss of the device or risk of information leakage.
- R2: The user should sign the confidentiality term or the term of non-disclosure agreement concerning the information that will be accessed and the compliance of his activities.
- R3: The user should authorize the installation of asset management software on his personal device, defined by the company, allowing the IT team to manage this device and to ensure control of the data stored in it.
- R4: The personal device used by the user should meet the minimum levels of security defined by the IT team. This evaluation may consider the software's version installed on the device, whether the device has been rooted, or if it has any software that does not comply with good security practices.
- R5: There should be an agreement between the company and the user concerning the use of the device outside of working hours and vacations, which may be regulated by security policies and monitored by a mobile device control tool.
- R6: The company should set Internet usage levels, depending on the user's role and need inside the program. This restriction can be defined and presented to the user during their enrollment in BYOD's program.
- R7: The company should implement policies to block access to wireless networks with low level of security, ensuring that the device will only access secure networks when out of the office.

- R8: The company should maintain control of devices compatible with the corporate technologies and infrastructure, denying any type of device that is incompatible or with incorrigible vulnerability.
- R9: The operating system installed on the device should be supported by the manufacturer. This measure ensures that the manufacturer still make security updates available for this device, ensuring continuous assessment and correction of vulnerabilities.

B. *Monitoring and maintenance step in BYOD's program*

As important as the user's commissioning in the good information protection practices mentioned in the previous subsection, this stage regards the maintenance of information protection, performing the monitoring and investigation of events, looking for identified incidents. The process of monitoring and maintenance of BYOD's program presented, focuses on adherence and ensure constant updating of standards, adapting them as the business demands. For the monitoring process, the framework suggests some actions based on ISO 27002:2005 [1] and in the CIS controls, that is:

- R1: Access to information and inclusion in security groups of a user who changes from company business areas should be updated to guarantee access to information and ability to execute activities related to his new responsibilities.
- R2: The company should offer recycling training in information security when it deems necessary, with a focus on updating users about some new technology or a process that needs to be implemented so that to ensure data security in the company.
- R3: The company should perform audits on access to sensitive files, correlating users, devices and tasks in order to look for possible information security incidents.
- R4: The company should implement logical protection, using the mobile device management tool, to secure corporate data that is in transit at employees' devices.
- R5: The company should provide an emergency contact to inform security incidents with devices covered by BYOD's policy. Unauthorized access to the data, device loss and theft are considered an incident.
- R6: The company should have a contingency plan to deal with the information security incident without impacting business.
- R7: The company should provide a backup tool and guide users to backup corporate data whenever possible. This measure guarantees the availability of the information in case of lost or robbery of mobile device.
- R8: The company should create an approval flow for security updates and monitor the success of applying these updates to BYOD devices.
- R9: The company should have a list of trusted corporate software available to users. This software should be managed by the IT team.

C. *Discharge step in BYOD's program*

BYOD's user's discharge process is extremely important compared to its predecessors. The program's decommissioning step does not occur only when the user leaves the company but can also occur when the business area understands that device access constrains are no longer necessary. The access revocation for user to carry out his activities is extremely important for the company, since it ensures that access is kept restricted to those interested and responsible for performing activities that need to handle this information. For the user disconnection process, the framework suggests some actions based on the ISO 27002:2005 [1] and the CIS controls [3]:

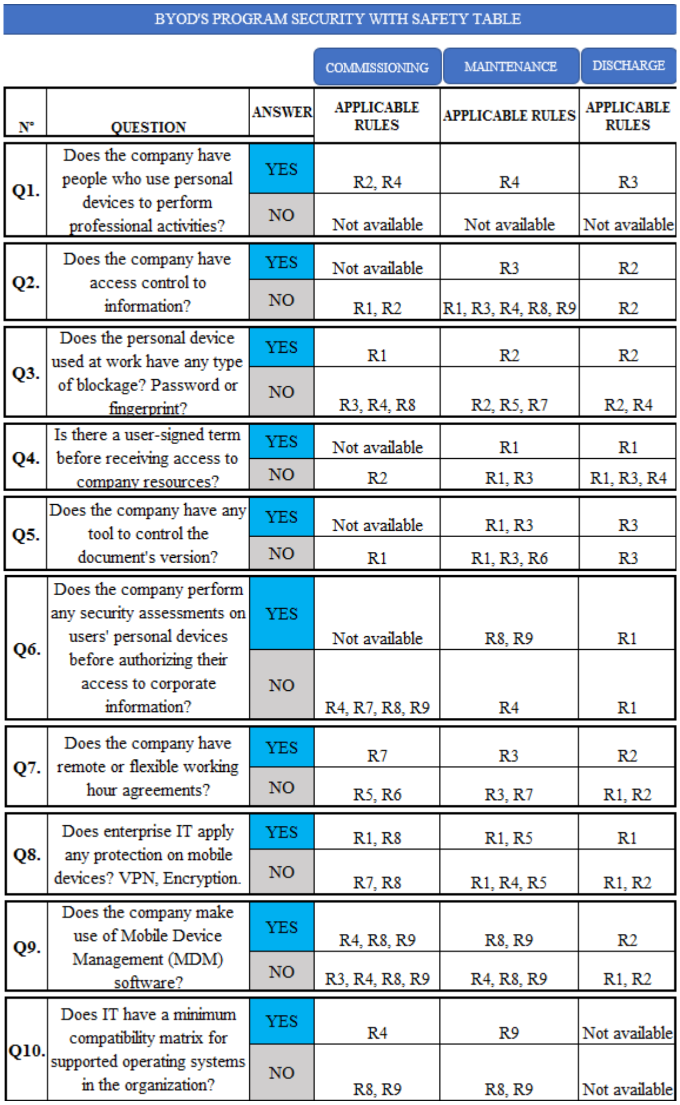
- R1: The revoke must be communicated by Human Resources before the contractual change or area movement. This early communication ensures that measures can be taken to ensure no leakage of restricted data that may be accessed by the user with his personal device.
- R2: The company should have a cryptographic protection process and remotely data destruction to be used in case of information security and user's disconnection in the company.
- R3: It should be kept audit records of file access during a period defined by the information security team for research purposes, even after the user removal from the program and its accesses have been revoked.
- R4: The company should have a defined process for discharge of BYOD's program, with defined responsibilities assigned to each area involved in this process.

D. *Evaluation template*

Considering the guidelines of BYOD's program, a survey was elaborated with questions about the routine of professionals who use personal devices inside the company. The survey must be answered by those responsible for the strategic area of the company and, through this form, an identified security risk analysis is presented. Moreover, the guidelines presented in this document may assist companies in the protection of sensitive data through personal devices.

The survey presented in table 3.1 is used in the case study to raise the adherence of companies with respect to information security practices aimed at BYOD devices. In this same table, the norms that apply to each scenario are presented, considering the positive or negative answer to the question.

Table 3.1 Questionnaire used in BYOD's case study.



BYOD'S PROGRAM SECURITY WITH SAFETY TABLE

			COMMISSIONING	MAINTENANCE	DISCHARGE
N°	QUESTION	ANSWER	APPLICABLE RULES	APPLICABLE RULES	APPLICABLE RULES
Q1.	Does the company have people who use personal devices to perform professional activities?	YES	R2, R4	R4	R3
		NO	Not available	Not available	Not available
Q2.	Does the company have access control to information?	YES	Not available	R3	R2
		NO	R1, R2	R1, R3, R4, R8, R9	R2
Q3.	Does the personal device used at work have any type of blockage? Password or fingerprint?	YES	R1	R2	R2
		NO	R3, R4, R8	R2, R5, R7	R2, R4
Q4.	Is there a user-signed term before receiving access to company resources?	YES	Not available	R1	R1
		NO	R2	R1, R3	R1, R3, R4
Q5.	Does the company have any tool to control the document's version?	YES	Not available	R1, R3	R3
		NO	R1	R1, R3, R6	R3
Q6.	Does the company perform any security assessments on users' personal devices before authorizing their access to corporate information?	YES	Not available	R8, R9	R1
		NO	R4, R7, R8, R9	R4	R1
Q7.	Does the company have remote or flexible working hour agreements?	YES	R7	R3	R2
		NO	R5, R6	R3, R7	R1, R2
Q8.	Does enterprise IT apply any protection on mobile devices? VPN, Encryption.	YES	R1, R8	R1, R5	R1
		NO	R7, R8	R1, R4, R5	R1, R2
Q9.	Does the company make use of Mobile Device Management (MDM) software?	YES	R4, R8, R9	R8, R9	R2
		NO	R3, R4, R8, R9	R4, R8, R9	R1, R2
Q10.	Does IT have a minimum compatibility matrix for supported operating systems in the organization?	YES	R4	R9	Not available
		NO	R8, R9	R8, R9	Not available

IV. Experiment Description

CONSIDERING the guidelines presented in the three stages of a user's life cycle within BYOD's program, the paper presents a case study to illustrate how such standards can help companies if applied throughout BYOD's culture implementation. The case study consists of analyzing three companies from different segments, one from the financial investment sector, the second from engineering area and the last from the leasing of shared office environments. All these companies allow users to use their own devices to perform professional activities.

For confidentiality purposes, this work will call the engineering firm as "A", the financial services consulting firm as "B" and the remote office firm as "R".

"A" is a small engineering company with an average of 50 employees, which operates in the state of Rio de Janeiro/Brazil providing technical assistance in the areas of engineering, economics, actuarial and finance. About 40% employees work in customer or out-of-office environments, requiring access to information stored inside the office. The company has an IT team that supports the search for security solutions and users support. Company "A" considers its IT infrastructure secure, as it has had no incidents related to information loss or leakage known in recent years.

"B" is a medium-sized investment consulting firm with approximately 100 employees and offices in Rio de Janeiro, São Paulo and Belo Horizonte, which advises on financial investments, supporting its clients in investment funds management and helping them to invest their income. The company has about 30% of its employees constantly in transit or in meetings outside the company facilities, and therefore, need access to the data stored in the Rio de Janeiro office. Company "B" has an IT support agreement with a third-party company and relies on the security of its customers' information.

"R" is a shared office leasing company with worldwide presence with about 3,000 spaces available to its customers. With around 8,000 employees, it offers a complete office infrastructure for its clients, including Internet connection. With multiple customers using corporate and personal devices to work, sharing the same Internet infrastructure, the company considers its infrastructure safe and professional.

With the survey filled out by the IT manager of company "A", it is possible to analyze in Table 4.1 the adherence to BYOD's framework with security standards. For each response presented, it is presented a set of rules adherent to the problem identified in the research, which address each identified risk.

Table 4.1 Result of the experiment with company "A"

BYOD Program			
Does the company have people who use personal devices to perform professional activities?			
Answer: YES	Program life cycles		
	Commissioning	Maintenance	Discharge
P1	R2, R4	R4	R3
Does the company have access control to information?			
Answer: YES	Commissioning	Maintenance	Discharge
P2	Not available	R3	R2
Does the personal device used at work have any type of blockage? Password or fingerprint?			
Answer: YES	Commissioning	Maintenance	Discharge
P3	R1	R2	R2
Is there a user-signed term before receiving access to company resources?			
Answer: NO	Commissioning	Maintenance	Discharge
P4	R2	R1, R3	R1, R3, R4
Does the company have any tool to control the document's version?			
Answer: YES	Commissioning	Maintenance	Discharge
P5	Not available	R1, R3	R3
Does the company perform any security assessments on users' personal devices before authorizing their access to corporate			

information?			
Answer: NO	Commissioning	Maintenance	Discharge
P6	R4, R7, R8, R9	R4	R1
Does the company have remote or flexible working hour agreements?			
Answer: NO	Commissioning	Maintenance	Discharge
P7	R5, R6	R3, R7	R1, R2
Does enterprise IT apply any protection on mobile devices? VPN, Encryption.			
Answer: NO	Commissioning	Maintenance	Discharge
P8	R1, R8	R1, R5	R1
Does the company make use of Mobile Device Management (MDM) software?			
Answer: NO	Commissioning	Maintenance	Discharge
P9	R3, R4, R8, R9	R4, R8, R9	R1, R2
Does IT have a minimum compatibility specification for supported operating systems in the organization?			
Answer: YES	Commissioning	Maintenance	Discharge
P10	R4	R9	Not available

With the survey filled out by the person in charge of company "B", it is possible to analyze at Table 4.2 the adherence to BYOD's framework with security standards presented in this article. For each response presented, a table was prepared with the rules that address each identified risk.

Table 4.2 Result of the experiment with company "B".

BYOD Program			
Does the company have people who use personal devices to perform professional activities?			
Answer: YES	Program life cycles		
	Commissioning	Maintenance	Discharge
P1	R2, R4	R4	R3
Does the company have access control to information?			
Answer: YES	Commissioning	Maintenance	Discharge
P2	Not available	R3	R2
Does the personal device used at work have any type of blockage? Password or fingerprint?			
Answer: YES	Commissioning	Maintenance	Discharge
P3	R1	R2	R2
Is there a user-signed term before receiving access to company resources?			
Answer: NO	Commissioning	Maintenance	Discharge
P4	R2	R1, R3	R1, R3, R4
Does the company have any tool to control the document's version?			
Answer: YES	Commissioning	Maintenance	Discharge
P5	Not available	R1, R3	R3
Does the company perform any security assessments on users' personal devices before authorizing their access to corporate			

information?			
Answer: NO	Commissioning	Maintenance	Discharge
P6	R4, R7, R8, R9	R4	R1
Does the company have remote or flexible working hour agreements?			
Answer: NO	Commissioning	Maintenance	Discharge
P7	R5, R6	R3, R7	R1, R2
Does enterprise IT apply any protection on mobile devices? VPN, Encryption.			
Answer: YES	Commissioning	Maintenance	Discharge
P8	R1, R8	R1, R5	R1
Does the company make use of Mobile Device Management (MDM) software?			
Answer: NO	Commissioning	Maintenance	Discharge
P9	R3, R4, R8, R9	R4, R8, R9	R1, R2
Does IT have a minimum compatibility specification for supported operating systems in the organization?			
Answer: YES	Commissioning	Maintenance	Discharge
P10	R4	R9	Not available

With the survey filled out by the IT manager of the company "R", it is possible to analyze in Table 4.3 the adherence to BYOD's framework with security standards presented in this work. For each response presented, a table was prepared with the rules that address each identified risk.

Table 4.3 Result of the experiment with company "R".

BYOD Program			
Does the company have people who use personal devices to perform professional activities?			
Answer: YES	Program life cycles		
	Commissioning	Maintenance	Discharge
P1	R2, R4	R4	R3
Does the company have access control to information?			
Answer: NO	Commissioning	Maintenance	Discharge
P2	R1, R2	R1, R3, R4, R8, R9	R2
Does the personal device used at work have any type of blockage? Password or fingerprint?			
Answer: YES	Commissioning	Maintenance	Discharge
P3	R1	R2	R2
Is there a user-signed term before receiving access to company resources?			
Answer: YES	Commissioning	Maintenance	Discharge
P4	Not available	R1	R1
Does the company have any tool to control the document's version?			
Answer: NO	Commissioning	Maintenance	Discharge
P5	R1	R1, R3, R6	R3
Does the company perform any security assessments on users'			

personal devices before authorizing their access to corporate information?			
Answer: NO	Commissioning	Maintenance	Discharge
P6	R4, R7, R8, R9	R4	R1
Does the company have remote or flexible working hour agreements?			
Answer: NO	Commissioning	Maintenance	Discharge
P7	R5, R6	R3, R7	R1, R2
Does enterprise IT apply any protection on mobile devices? VPN, Encryption.			
Answer: NO	Commissioning	Maintenance	Discharge
P8	R7, R8	R3, R7	R1, R2
Does the company make use of Mobile Device Management (MDM) software?			
Answer: NO	Commissioning	Maintenance	Discharge
P9	R3, R4, R8, R9	R4, R8, R9	R1, R2
Does IT have a minimum compatibility specification for supported operating systems in the organization?			
Answer: YES	Commissioning	Maintenance	Discharge
P10	N8, N9	N8, N9	Not available

This experiment identified that company "A", even investing in corporate information protection technologies, does not have centralized management of its users' BYOD devices. This company also does not have a formalized contract that allows sharing the responsibility of not leaking corporate information, exposing itself to serious risk of losing the important information. For these risks, the framework proposed in this work presents the rule R2 inside the commissioning cycle that suggests the signature of terms of confidentiality and responsibility of the user with the information under their responsibility, being able to respond legally in case of misuse of these resources. The framework also suggests on rule R3 at monitoring cycle that the company should keep monitoring access of sensitive data to help tracking and correcting the misuse of these sensitive data by non-authorized personal. The framework presents rule R3 at discharge cycle that companies keep audit records for further investigations in case of security incidents to help charging who's responsible for the issue.

Like company "A", company "B" also do not have responsibility contracts signed by user with the access granted to information. Company "B" also has no audit and control versioning of documents, making it impossible to trace, or even protect, information and ensure the original version at any given time. The company does not have documents or tools that control the use of personal devices outside working hours and exposes itself form being sued in labor court. Considering the risks presented above, BYOD's framework suggest the rules R1 and R3 at monitoring cycle to keep track of security access groups and sensitive files access to mitigate, and even eliminate these risks, explaining how the company should proceed to treat the identified failures and protect their intellectual property. On rule 3 at discharge cycle, the framework suggests that these tracking records should be kept for long term to help investigate possible future issues.

During this research, it was identified that the company "R" has no monitoring of the devices connected to its infrastructure. The company also has no network usage agreements, as well as encryption and VPN for providing only on-site access to its customers. BYOD's framework provides rules R7 and R8 at commissioning cycle, providing best practices to apply security policies to BYOD devices in order to protect it from non-security wireless networks outside the corporation or even denying the ingress of devices without it's vendor support. The rules R3 and R7 sugests the use of tools to protect and monitor access to sensitive data stored on BYOD devices. The rules R1 and R2 at discharge cycle provide actions that help prevent the misuse of sensitive data when the device is stolen, lost or being removed from the BYOD program. These security rules presented in this work provides the help to support implementation and maintenance of measures to protect the information of the company and its customers.

Based on the information analyzed above, it was possible to map information security vulnerabilities in the three experienced companies. In each survey's question, BYOD framework shows the rules that are applicable to the identified risks, being able to mitigate and even eliminate the risk in some cases. Whenever IT environment already has good security practices for implemented BYOD devices, user maintenance and discharge rules still apply, thus ensuring that the user device life cycle in the program is followed.

The surveys presented in this paper show the risks that companies are exposed. Through the information collected in the surveys, it is possible to identify the vulnerabilities and propose the implementation of the advices from BYOD's framework with security. It safely proposes control of BYOD's device lifecycle using its three cycles: commissioning, maintenance and discharge of BYOD's device. With the standards presented in these three cycles, it is possible to treat the identified vulnerabilities by applying good information security practices based on ISO 27002:2005 and the practical CIS information security controls directed to BYOD's platform.

V. Conclusion

THIS research aimed to study the challenges of protecting sensitive data in corporations that have adopted BYOD's culture and presented guidelines to protect the company's confidential information based on good information security management practices contained in ISO 27002:2005 and in the information security controls defined by the CIS.

This paper shows some points where traditional information security policies do not effectively protect companies and users that use personal devices in the execution of corporate activities. With the vulnerabilities identified, it is proposed a framework based on the best information security practices of ISO 27002:2005 and CIS information security controls, in the life cycle format of BYOD's program, so that it is possible to meet the needs of these companies that adopt such culture. To test the framework and its rules in a real environment, three companies were analyzed through a survey with ten questions regarding the use of BYOD devices, where each question has an associated risk and norms to handle both the positive and negative answers. At the end of the experiment, an analysis of the information collected in the three companies is presented and BYOD's framework rules are presented for each identified risk. Each rule presented in the three cycles of the framework offers good practices on how to mitigate and to eliminate.

With the increase in the use of personal devices to perform work tasks, there is also growing concern about the protection of these devices by the IT staff. The constant evolution of technologies, bring great challenges to companies when they need to adapt and remain competitive in the market. The security of the intellectual property of these companies must be considered with extreme importance, or improper access can generate irreparable damage to the company image.

Each day, new variations of BYOD's culture arise, and these alternatives have the same goal as BYOD, to improve the ease of use of a device in the company, increasing the efficiency and user satisfaction in their work environment. From the variations of BYOD, it can be mentioned: (1) Choose Your Own Device (CYOD), which allows the user to choose a device from a list previously approved by the IT team; (2) Company Owned, Personally Enabled (COPE) that makes available to use personal applications, and to store information that is not of corporate use; (3) Corporate Liable Employee Owned (CLEO), which is considered a more democratic BYOD, where there is an agreement of freedom of choice of the device and internet plans between the user and the company. For the variations listed above, it is necessary to create information security processes and policies with focus on monitoring the evolution of technology and the market without jeopardizing the intellectual good of the company. As future works, it is interesting to evolve the suggested policies for the use of BYOD in the new alternatives such as CYOD, COPE and CLEO.

VI. References

[1] ABNT NBR ISO/IEC 27002:2005. "Code of practice for the management of information security". in: http://www.fieb.org.br/download/senai/NBR_ISO_27002.pdf. Pages 22 and 23. August 16th, 2018.

[2] VERT Technology. "CYOD, COPE and CLEO: Know the alternatives to BYOD". In: http://www.vert.com.br/blog-vert/cyod-cope-e-cleo-conheca-as-alternativas-ao-byod/. September 13th, 2018.

[3] CIS Critical Security Controls. "CIS Control – Procedures and tools". In: https://web.archive.org/web/20160809003039/https://www.cisecurity.org/critical-controls/documents/CSC-MASTER-VER%206.0%20CIS%20Critical%20Security%20Controls%2010.15.2015.pdf . October 10th 2018.

[4] GAJAR, Prashant Kumar, GOSH, Arnab, RAI, Shashikant. "Bring Your Own Device (BYOD): Security Risks and Mitigating Strategies". In: http://jgrcs.info/index.php/jgrcs/article/view/654/477/. October 11th, 2018.

[5] ZAHADAT, Nima, BLESSNER, Paul, BLACKBURN, Timothy, OSLON, Bill A. "BYOD security engineering: A framework and its analysis". October 11th, 2018. DOI: 10.1016/j.cose.2015.06.011

[6] RIVERA, David, GEORGE, Geethu, PRATHAP, Peter, MURALIDHARAM, Sahithya, KHANUM, Sumaya. "Analysis of Security Controls for BYOD". October 11th, 2018. URI: http://hdl.handle.net/11343/33338

[7] ALHARTHY, Khoula, SHAWKAT, Wael. "Implement Network Security Control Solutions in BYOD Environment". October 13th, 2018. DOI: 10.1109/ICCSCE.2013.6719923

[8] ALI, Sara, QURESHI, Muhammad Nauman, ABASSI, Abdul Ghafoor. "Analysis of BYOD Security Frameworks". October 13th, 2018. DOI: 10.1109/CIACS.2015.7395567

[9] PENG, Wei, LI, Feng, HAN, Keesook J., ZOU, Xukai, WU, Jie. "T-dominance: Prioritized Defense Deployment for BYOD Security". October 13th, 2018. DOI: 10.1109/CNS.2013.6682690

[10] ARMANDO, Alessandro, COSTA, Gabriele, MERLO, Alessio, VERDERAME, Luca, WRONA, Konrad. "Developing a NATO BYOD Security Policy". October 13th, 2018. DOI: 10.1109/ICMCIS.2016.7496587

[11] LEE, Ji-Eun, PARK, SE-HO, YOON, Hyoseok. "Security Policy based Device Management for Supporting Various Mobile OS". October 13th, 2018. DOI: 10.1109/ICCTIM.2015.7224611

[12] LEE, Jaeho, LEE, Yongjin, KIM, Seung-Cheon. "A White-List Based Security Architecture (WLSA) for the Safe Mobile Office in BYOD's Era". October 13th, 2018. DOI: 10.1007/978-3-642-38027-3_98

[13] BELLO, Abubakar Garba, MURRAY, David, ARMAREGO, Jocelyn. "A systematic approach to investigating how information security and privacy can be achieved in BYOD environments". October 13th, 2018. DOI: 10.1108/ICS-03-2016-0025

Ulysses Moreira da Neves received his MBA in Systems and Computing Engineering from the Federal University of Rio de Janeiro - UFRJ (2018), certified in information security foundation based on ISO IEC 27002 (2015), Microsoft MCSE (Microsoft Certified Solutions Expert) in Cloud Computing and Associate degree in IT Management from the University Paulista - UNIP (2016).

He currently works with Storage and Microsoft technology at Fundação Getúlio Vargas, a large company in the education industry, having participated in works in private and public cloud computing (Azure), datacenter consolidations, security in bring your own device, and applications management.

Flávio Luis de Mello received his DSc. in Theory of Computation and Image Processing from the Federal University of Rio de Janeiro - UFRJ (2006), MSc. in Computer Graphics from the Federal University of Rio de Janeiro - UFRJ (2003), Undergraduate degree in Systems Engineering from the Military Institute of Engineering - IME (1998).

He developed command and control systems and implemented military messages interchange applications during twelve years as a Brazilian Army officer. He was responsible for developing software applications based on machine learning and knowledge reasoning from Mentor Group.

Dr Mello currently is Associate Professor at the Electronic and Computer Engineering Department (DEL) of Polytechnic School (Poli) at the Federal University of Rio de Janeiro (UFRJ). He is head of the Machine Intelligence and Computing Models Laboratory (IM2C).