UNIVERSIDADE ESTADUAL DO SUDOESTE DA BAHIA
DEPARTAMENTO DE CIÊNCIAS EXATAS E TECNOLÓGICAS
COLEGIADO DO CURSO DE CIÊNCIA DA COMPUTAÇÃO

TAMARA RITIELLE SOARES FROTA

GESTÃO DA SEGURANÇA DA INFORMAÇÃO DA UESB: A VISÃO DO USUÁRIO

Vitória da Conquista
2017

TAMARA RITIELLE SOARES FROTA

GESTÃO DA SEGURANÇA DA INFORMAÇÃO DA UESB: A VISÃO DO USUÁRIO

Monografia apresentada à banca examinadora da Universidade Estadual do Sudoeste da Bahia, como requisito parcial para a obtenção do grau de Bacharel em Ciência da Computação.

Orientador: Prof. Dr. Hélio Lopes dos Santos.

Coorientadora: Profa. Dra. Cátia Mesquita Brasil Khouri

Vitória da Conquista

2017

TAMARA RITIELLE SOARES FROTA

GESTÃO DA SEGURANÇA DA INFORMAÇÃO DA UESB: A VISÃO DO USUÁRIO

Aprovado em ___ / ___ / _____

BANCA EXAMINADORA

_____

Orientador: Prof. Dr. Hélio Lopes dos Santos.

Universidade Estadual do Sudoeste da Bahia – UESB

_____

Coorientadora: Profa. Dra. Cátia Mesquita Brasil Khouri.

Universidade Estadual do Sudoeste da Bahia – UESB

_____

Profa. Dra. Maísa Soares dos Santos Lopes.

Universidade Estadual do Sudoeste da Bahia – UESB

Dedico este trabalho a Deus, aos meus pais, Jaime e Luzia, à minha irmã, Tamilles e todas as pessoas que me ajudaram no desenvolvimento desta monografia. Maone e sua família, que me adotaram nesta etapa final e à sua mãe, tia “Sibila”, pela banca examinadora precedente. Aos colegas de curso pela paciência. A Sid Gubert, por toda colaboração e disposição dada a mim. Aos meus orientadores Hélio Lopes e Cátia Khouri.

Minha gratidão a todos vocês!

“Spirit lead me where my trust is without borders
Let me walk upon the waters
Wherever you would call me
Take me deeper than my feet could ever wander
And my faith will be made stronger
In the presence of my savior “

(Hiilsong United)

RESUMO

Os ativos de tecnologia da informação de uma organização, são os itens mais cobiçados e que necessitam de atenção dos demais. A segurança da informação (SI) trata dos cuidados que são necessários para que estes ativos estejam protegidos de acessos indevidos, alterações indesejadas, e sua não disponibilidade. Como parte deste sistema de defesa, o usuário é a primeira barreira de proteção, e sua função dentro do Sistema de Gestão da SI é inerente a todo o aparato tecnológico de proteção. Não há tecnologia de segurança suficiente para salvaguardar os dados de uma empresa, se seus usuários estiverem despreparados. Pessoas mal-intencionadas usam da Engenharia Social para obter informações sigilosas, cujas técnicas, estão evoluindo e disseminando cada vez mais. Na tentativa de estar munidos contra os ataques que envolvem diretamente seus colaboradores, as organizações precisam adotar práticas preventivas e corretivas, e disseminá-las dentro do ambiente de trabalho. A respeito desta temática, este trabalho mostra como os funcionários da Universidade Estadual do Sudoeste da Bahia (UESB) desempenham seu papel de proteção, ou não, dentro da SI da instituição. A pesquisa foi desenvolvida sobre um levantamento de dados, que teve como público alvo os funcionários da UESB Campus Vitória da Conquista que fazem uso de sistema interno ou tecnologia da informação para realizar suas atividades na instituição. Após análise dos resultados, foram listadas ações positivas e negativas, seguidas de sugestões de melhorias. O resultado indica que os funcionários da UESB não estão preparados para desempenhar o seu papel dentro da SI.

Palavras-chave: engenharia social, política de segurança da informação, segurança da informação.

ABSTRACT

The information technology assets of an organization are the most coveted items that need attention from others. Information security (IS) deals with the care that is necessary for these assets are protected from unauthorized access, unwanted changes, and its non-availability. As part of this defense system, the user is the first protection barrier, and its function in the IS Management System is inherent to the entire technological protection apparatus. There is not enough security technology to protect the data of a company, if your users are unprepared. Malicious people use Social Engineering to get confidential information, whose techniques are evolving and increasingly widespread. In an attempt to be armed against attacks that directly involve their collaborators, organizations need to adopt preventive and corrective practices, and disseminate them at the work environment. Regarding this issue, this paper shows how the employees of the State University of the Southwest of Bahia (UESB) perform their function of protection, or not, in the IS of the institution. The research was developed on a survey of date, which had as target audience the employees of UESB Campus Vitória da Conquista that make use of internal system or information technology to carry out its activities in the institution. After analyzing the results, positive and negative actions are listed, followed by suggestions for improvements. The result indicates that UESB employees are not prepared to perform their function in the IS.

Keywords: social engineering, information security policy, information security.

LISTA DE ABREVIAÇÕES

Cetic.br	Centro de Estudos sobre as Tecnologias e da Comunicação
ES	Engenharia Social
GSI	Gestão da Segurança da Informação
PSI	Política de Segurança da Informação
REDA	Regime Especial de Direito Administrativo
SGSI	Sistema de Gestão da Segurança da Informação
SI	Segurança da Informação
UESB	Universidade Estadual do Sudoeste da Bahia

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

> "Quando os empregados de confiança são enganados, influenciados ou manipulados para revelar informações sigilosas ou para executar ações que criem um buraco na segurança para que o atacante se infiltre, nenhuma tecnologia do mundo pode proteger uma organização." (MITINICK & SIMON, 2005)

Quando se trata da Segurança da Informação (SI), a ideia que se tem é de um aparato de equipamentos e softwares de última geração habilitados para um possível ataque indesejado de crackers. Contudo, conforme destacado por Mitnicik e Simon (2005), é de extrema importância que a organização invista na qualificação dos seus colaboradores, no intuito de mitigar métodos que possam acarretar na quebra da segurança.

Um usuário despreparado, pode gerar uma série de problemas para a confidencialidade das informações da organização. Segundo Rocha (2008), o usuário é o elo mais fraco no processo de segurança, todavia, é o responsável por garantir a fidelidade das informações. Assim sendo, a ideia inicial de tornar a organização imune a ataques com artefatos padrões de SI, acaba sendo um pensamento equivocado.

Nos últimos anos, a eclosão de notícias a respeito do vazamento de informações em entidades públicas nacionais, vêm se tornando mais frequentes. Casos notáveis como o da Petrobrás em 2008[1] e o da CIA em 2013[2], envolveram importantes corporações que possuíam um conjunto tecnológico para a proteção da informação pronto para lidar com falhas na SI e apesar disto, contrariedades ocorreram. Haja vista, as falhas não foram ocasionadas pelo fator tecnológico.

A SI depende de fatores que funcionam de forma síncrona, um fator dependendo do outro. O fator físico (equipamentos), lógico (software), humano (usuário) atuam de forma conjunta, de modo que a eficiência de um está estreitamente ligada com a eficiência do outro. Além destes fatores, a SI depende também da gestão Da organização, que deve ocupar-se dos riscos, da continuidade das tarefas, do controle de acesso, e do local de aprovisionamento dos ativos.

---

[1] https://oglobo.globo.com/economia/roubo-de-dados-da-petrobras-foi-espionagem-diz-pf-3632874
[2] http://glo.bo/19Rj2g6

O fator humano por se tratar de questões comportamentais, práticas simples e de conscientização, é o fator que menos há investimentos por parte das organizações. Justamente por se tratar do grupo mais fraco dentro da SI das organizações, é o grupo que mais sofre ameaças e vulnerabilidades no sistema.

Em função dessas questões que envolvem a SI, este trabalho apresenta um levantamento de dados sobre a SI na Universidade Estadual do Sudoeste da Bahia (UESB), tendo como objeto de pesquisa, o papel dos colaboradores da instituição dentro do Sistema de Gestão da Segurança da Informação (SGSI) e se estes estão preparados para desempenhá-lo.

O presente documento tem como propósito apresentar o trabalho de conclusão de curso da graduanda Tamara Ritielle Soares Frota, com a principal área de concentração da monografia a Ciência da Computação, subárea SI do ponto de vista do usuário

1.1 Problema de Pesquisa

Em toda organização, seja ela privada ou pública, é de extrema importância a proteção de seus ativos de tecnologia da informação, tendo como um dos mais relevantes, a Informação. A SI trata de medidas que previnem possíveis falhas na proteção dos dados de uma organização.

Toda essa segurança não se estende somente a questões tecnológicas, vai além de equipamentos e envolve o fator humano, fator este que pode fazer com que qualquer outra medida preventiva seja eficiente ou não.

Levando em consideração o papel do usuário nos métodos de proteção dos ativos de tecnologia de uma organização, a pesquisa busca problematizar a questão: Os usuários da Universidade Estadual do Sudoeste da Bahia (UESB) estão preparados para desempenhar o seu papel no processo de proteção das informações da instituição?

1.2 Hipótese

A importância do papel do usuário na SI, levanta a seguinte hipótese: os usuários da UESB não estão preparados para contribuir adequadamente com a SGSI da instituição.

Se a instituição investe em treinamentos, campanhas educativas e divulgação, o resultado deste processo são funcionários mais preparados e conscientes de suas ações sobre a SI da organização.

Desta maneira, usuários conscientes conseguem desempenhar suas funções dentro do processo da SI. Esta consciência precisa ser desenvolvida dentro da organização, com campanhas de conscientização, campanhas de incentivos e com a divulgação da política de segurança interna. Sem essas práticas por parte da organização, o usuário não poderia exercer o seu real papel dentro de todo o SGSI.

1.3 Motivação

A motivação deste trabalho se iniciou a partir da análise de casos notáveis de falhas na SI, ocorridas em importantes instituições como Petrobrás em 2008, CIA em 2013 e um próprio episódio ocorrido na UESB em 2016, cujo site foi utilizado por pessoas não autorizadas para publicação de uma nota de repúdio às invasões escolares e em instituições públicas. Através desta observação, manifestou-se a necessidade de uma reflexão sobre por quais razões tais falhas teriam ocorrido, se por falta de investimento em tecnologia, escassez ou inexistência de treinamento e conscientização dos usuários do sistema, ou ainda, se por negligência.

1.4 Objetivo geral

O presente trabalho tem o intuito de mostrar um estudo na SI da Universidade Estadual do Sudoeste da Bahia (UESB) e avaliar se os seus funcionários estão devidamente preparados para desempenhar o seu papel dentro do SGSI da instituição.

1.5 Objetivos específicos

Entre os objetivos específicos estava o de verificar se o usuário possui consciência dos riscos que podem trazer para a SI da organização; verificar se o usuário executa ações que são consideradas boas práticas para manter a SI da universidade e sugerir possíveis melhorias que irão contribuir para a SI da organização.

1.6 Organização da Monografia

Esta monografia encontra-se dividida em cinco capítulos. A primeira parte, seção introdutória, demonstra os objetivos e a motivação do trabalho, juntamente com a problemática que desenvolveu os estudos da pesquisa.

O segundo capítulo, apresenta o estado da arte, uma descrição de como se encontra os estudos acerca da SI, numa visão geral.

O terceiro capítulo apresenta as referências teóricas que fundamentaram o estudo da SI da UESB, que foi objeto de pesquisa da monografia.

O quarto capítulo explora todo o desenvolvimento da pesquisa. Relata a metodologia utilizada, o procedimento de pesquisa adotado para obtenção dos dados, e uma análise dos dados obtidos na aplicação.

O quinto capítulo faz inferência aos dados obtidos, e demonstra sugestões de práticas possíveis para sanar os problemas encontrados na SI da UESB. O último capítulo elenca as referências bibliográficas.

2. REVISÃO BIBLIOGRÁFICA

De acordo com a norma ISO/IEC 27002 (2005), a informação é um ativo de tecnologia, que assim como outros do mesmo grupo, precisam de proteção adequada. É um ativo de extrema importância para os negócios, haja vista o ambiente dos negócios, cada vez mais conectado, e por isso, é passível de sofrer um grande número de ameaças e vulnerabilidades.

Longo (s.d.) descreve que a preocupação com a segurança no âmbito computacional, nasceu do surgimento de máquinas de tempo compartilhado, time-sharing, que são máquinas que permitem que mais de um usuário/pessoa faça o uso do computador ao mesmo tempo. Ainda segundo Longo (s.d.), foi somente no ano de 2000 que foi publicada a primeira norma internacional sobre SI.

Segurança é o estado, qualidade ou condição de uma pessoa ou coisa que está livre de perigos, de incertezas, assegurada de danos e riscos eventuais, afastada de todo mal. (HOUAISS, 2001, p. 2536)

Para Fontes (2006 apud ROCHA, 2008) SI é composta de orientações, normas, procedimentos, políticas e práticas que visam assegurar os ativos de tecnologia da informação, tornando possível a execução das atividades da organização, sem que haja perdas.

Conforme os procedimentos para segurança dos ativos da tecnologia da informação evoluíam, novas técnicas para burlar tais procedimentos surgiam. Em trabalho publicado por Rocha (2008), ele afirma que toda “corrente” costuma se partir do lado que o elo mais fraco se encontra e, para ele, o elo mais fraco é o usuário. O usuário é alvo de ataques e consequentemente de estudos.

Um dos maiores problemas enfrentados pelo elo mais fraco do SGSI, se não o principal problema, é a Engenharia Social (ES). De acordo Martins (2008), o termo “Engenharia Social” tornou-se popular após os estudos do hacker chamado Kevin Mitnick, no ano de 1990.

A ES usa da persuasão para conseguir informações restritas e acesso não autorizado a computadores, em alguns casos, aproveitando da confiança e inocência do funcionário da organização vítima (NBSO,2004, apud ROCHA, 2008).

“A verdade é que não existe uma tecnologia no mundo que evite o ataque de um engenheiro social. ” (MITNICK & SIMON, 2003, p.195). Mitnick e Simon (2003), afirmam que as tecnologias de segurança podem dificultar formas de ataques,

retirando o usuário da tomada de decisão. Ele afirma também, que a única forma de amenizar os riscos da ES na organização é através da conscientização dos colaboradores, aliado com a Política da Segurança da Informação (PSI) contendo normas que descrevam o comportamento do usuário, treinamento e educação.

2.1 Gestão da Segurança da Informação

Nesta seção serão descritos os conceitos de elementos das subáreas da SI nos quais este trabalho se baseou

2.1.1 Informação

A Informação sempre foi objeto de estudo e cobiça da sociedade, desde os tempos da II Guerra Mundial, em que a informação era tratada como algo extremamente valioso (CAPURRO & HJOLARD, 2003). Para Silva Filho (2008), a informação é qualquer conteúdo que pode ser armazenado ou compartilhado de algum modo, sendo assim, a informação pode vir por meio do pensamento, por escrita ou por meio digital, podendo ser manipulada de diferentes formas.

Para Lancaster (1989 apud MESSIAS, 2005), o conceito de informação é difícil de definir, podendo ter significados adversos e, naturalmente, ela terá significado diferente para pessoas diferentes. Para a SI, a informação, é o principal e mais valioso ativo, levando-se em consideração o mundo competitivo e globalizado atual (BAHIA. Normas de Segurança da Informação, 2015).

2.1.2 Segurança da Informação

”Segurança da Informação (SI) é a proteção da informação contra vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.” (BRASIL. Norma ISO/IEC 27002 – 2005).

Para esta Norma, é papel da SI tentar manter, de todas as formas possíveis, a informação protegida. SI abrange desde aspectos físicos como proteção dos ativos da informação, restrição de acesso aos terminais; aspectos lógicos, utilização de softwares para proteção e equipamentos tecnológicos; até aspectos humanos, como comportamento, treinamento e conhecimento do usuário.

Existem normativas que especificam as práticas necessárias para que a organização obtenha uma SI de sucesso. As normas ISO/IEC 27001 e ISO/IEC 27002

ditam medidas protetivas e preventivas que visam o sucesso da SI da organização, seja ela pública ou privada.

Para o estado da Bahia, existem ainda mais 17 normas que orientam os gestores de organizações que integram a administração pública do estado, as quais visam auxiliar a organização na proteção dos seus ativos de tecnologia, missão que se faz cada vez mais necessária. (BAHIA. Normas de Segurança da Informação, 2015)

Além das normativa, no estado da Bahia, é realizada a cada ano uma pesquisa de maturidade utilizada pelo Governo da Bahia para medir o nível de seguridade das instituições públicas do Estado (Anexo 2). Esta pesquisa tem como público alvo os gestores de tecnologia das instituições públicas do estado. O procedimento de pesquisa adotado é um questionário, que aborda sobre normas, práticas e ativos de tecnologia usados na SGSI.

A SGSI engloba um conjunto de medidas para que a organização minimize os prejuízos na execução do seu papel e de suas atividades. Segundo Fontes (2006 apud ROCHA, 2008), a proteção dos ativos de tecnologia da informação visa garantir alguns princípios:

- Confidencialidade: a informação só deve ser acessada por pessoal autorizado e que necessite da mesma para execução de sua atividade na organização;
- Integridade: a informação não deve ser alterada de modo que altere sua verdade;
- Auditabilidade: o uso e acesso da informação tem que estar disponível, identificando o autor do acesso e suas ações.
- Disponibilidade: a informação deve estar disponível, visando o bom funcionamento das atividades da organização;
- Não repúdio de autoria: o usuário que gerou ou alterou a informação não deve poder negar o fato, pois o mesmo pode ser comprovado através da auditabilidade.
- Legalidade: a informação deve respeitar as normas de regulamento da organização e sociedade.

2.1.3 O papel do usuário na segurança da informação

“Segurança tem início e termina nas pessoas. ”

Ellen Frisch

A SI de uma organização depende não somente de fatores tecnológicos e técnicos, mas também da maneira como o usuário trata a informação. Alguns casos de falhas na segurança da informação relatados na literatura ocorreram por questões relacionadas ao usuário (ROCHA, 2008), tornando irrelevante, neste aspecto, a utilização de equipamentos e softwares de última geração, sem que haja um usuário habilitado.

O usuário precisa estar consciente do seu papel dentro do SGSI da organização, e a par das consequências que podem ser geradas em decorrência do descumprimento das especificações das normas internas. O colaborador é o primeiro obstáculo contra possíveis invasões à SI da organização, logo, a disseminação da cultura da segurança da informação é de fundamental importância.

> "Se os funcionários, fornecedores e terceiros não forem conscientizados das suas responsabilidades, eles podem causar consideráveis danos para a organização. Pessoas motivadas têm uma maior probabilidade de serem mais confiáveis e de causar menos incidentes de segurança da informação. " (Norma ISSO/IEC 27002 – 2005, p.28)

Existem diversos casos de falhas ocorridas na SI de renomadas empresas do cenário mundial. No Brasil em 2008[3], a estatal Petrobrás notificou que teria sido vítima de um crime de espionagem industrial, após ter dados sigilosos de uma pesquisa divulgados em público.

Após uma investigação, a Polícia Federal constatou que não se tratava de um crime de espionagem industrial, e sim crime comum, com subtração de equipamentos furtados durante o seu transporte. O grande problema foi a forma escolhida para o transporte dos equipamentos, sem que houvesse as devidas precauções para ativos de tecnologia que continham dados sigilosos.

No cenário internacional em 2013[4], Edward Snowden, ex-funcionário da CIA, revelou informações que eram secretas da companhia. Edward foi acusado de espionagem, roubo e conversão de propriedade do estado. A ação do ex-funcionário revelou práticas consideradas abusivas por ele e atividades de espionagem em um âmbito mundial.

[3] https://oglobo.globo.com/economia/roubo-de-dados-da-petrobras-foi-espionagem-diz-pf-3632874
[4] http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html

O usuário influencia tanto fazendo parte da organização, quanto já estando fora dela. De acordo com as Normas de Segurança da Informação (BAHIA. Normas de Segurança da Informação, 2015), o usuário desempenha um papel de grande relevância em todas as etapas das práticas necessárias para o sucesso da SI.

De acordo a Mitnick e Simon (2003), uma empresa pode adquirir os melhores equipamentos e serviços de segurança que o recurso financeiro possa comprar, pode dispor de quadro de funcionários altamente treinados, ainda assim, essa empresa estará vulnerável. Entretanto, o comportamento do usuário dentro do sistema de proteção pode reduzir substancialmente essa vulnerabilidade.

2.1.4 Engenharia Social

Segundo Sassa (2001, apud ROCHA, 2008), o usuário é o elo mais frágil e mais fácil para a entrada e acesso às informações de uma organização, e é neste ponto que a Engenharia Social (ES) atua. A ES se ocupa em analisar o comportamento humano e a partir disso, pensar em formas de ataque para obter informações sobre algo que é sigiloso, através de técnicas para enganar as pessoas e convencê-las de que o engenheiro é uma pessoa que na verdade não é (MARTINS, 2008).

A ES analisa os traços comportamentais e psicológicos do usuário no sentindo de assim elaborar estratégias para manipulá-lo. Segundo Konsultex (2004, apud PEIXOTO, 2006), a ES é a ciência que estuda como o conhecimento do comportamento humano pode ser utilizado para induzir uma pessoa a atuar segundo o seu desejo.

De acordo com Peixoto (2006), a ES não é um processo de hipnose ou de controle da mente, mas as técnicas da ES são bastante usadas por detetives e magistrados, para se obter informações e confirmar a veracidade de uma fala.

Os ataques do engenheiro social podem aparecer através de uma ligação por telefone ou chat, passando-se por alguém que na verdade não é; pela rede, com sites maliciosos ou e-mails falsos e pessoalmente, através da persuasão, espiando “por cima dos ombros” ou capturando o microcomputador de algum usuário. O engenheiro social se articula de modo a esconder a subtração de informações, situação que nem sempre o usuário percebe, podendo assim, inocentemente ser manipulado.

Mitnick e Simon (2003) afirmam não existir uma tecnologia capaz de conter os ataques por parte da ES, porém o que se pode fazer são estudos e aprimoramento contínuos, para que os funcionários da organização estejam sempre preparados para lidar com as situações, na medida em que as técnicas da ES evoluem.

2.1.5 Política de Segurança da Informação

Com a crescente evolução da tecnologia e de formas variadas de comunicação, cada vez mais as organizações se tornam vulneráveis a ataques e roubos de informação. Juntamente com este crescimento, é necessário evoluir nos cuidados e atenção à segurança dos dados da organização.

É sabido que o usuário é, sim, uma peça chave na segurança, e que é a partir dele que todo o processo de segurança se torna eficiente. A ES evolui de acordo com o comportamento humano, fazendo-se necessário tratar os critérios de proteção dos dados como um fator também em constante evolução (FONSECA, 2009).

O conjunto de orientações e cuidados, sobre a SI é chamado de Política de Segurança da Informação (PSI) da organização. Seu principal papel é implementar, operar, aprimorar, estabelecer, fazer uma análise crítica de todo o Sistema de Gestão da Segurança da Informação (BRASIL. Norma ISO/IEC 27002 – 2005).

Cada organização possui uma PSI única que encaixe nas suas necessidades e dentro do seu orçamento, conforme o seu tipo de empresa, o tipo de informação, o nível crítico dessas informações e as atividades de seus colaboradores. De acordo com Fonseca (2009), as PSI precisam ser claras, de modo que os usuários entendam, com exatidão, a importância de cumpri-las sem que haja uma carga de insatisfação com a situação. Em suma, a PSI é um conjunto de boas práticas para a SI, aplicáveis para o usuário.

Ainda segundo Fonseca (2009), uma organização que possui e executa a PSI, estará menos susceptível a falhas na SI. Os seus usuários estarão mais preparados para situações de riscos, e consequentemente a cultura de SI estará difundida dentro dessa organização. As normas ISO/IEC 27001 e ISO/IEC 27002 se referem a práticas e medidas necessárias para se garantir a segurança dos ativos de tecnologia de uma organização. Tais normas, descrevem detalhadamente cada setor que compõe a SI.

2.2 Trabalhos Relacionados

Serão apresentados nesta seção, alguns trabalhos produzidos por profissionais da área que possuem tema semelhante ao proposto por este trabalho.

- **Pesquisa Cetic.br**

O Centro de Estudos sobre as Tecnologias da Informação e da Comunicação (Cetic.br), realizou uma pesquisa em 2013[5] e constatou que de 1.586 órgãos públicos federais e estaduais que declararam utilizar computador nos últimos 12 meses, 15% não possuem uma (PSI).

Embora seja um percentual pequeno, em se tratando de SI, é um índice que pode apontar uma grande vulnerabilidade. Para Fonseca (2009), a PSI possui instruções claras que orientam os funcionários a terem comportamentos que protejam as informações da organização, ademais de ser um elemento primordial no processo de proteção contra invasões ou ataques.

Em outra pesquisa da Cetic.br, realizada em 2015[6], publicada na Veja[7], foram examinados 1.644 órgãos públicos federais e estaduais que utilizaram práticas de SI nos últimos 12 meses. Dos quesitos avaliados, aquele que obteve menor índice positivo, foi o item sobre o suprimento de energia aos servidores centrais. 22% dos órgãos afirmaram não ter uma fonte extra de energia, por conseguinte, uma falha na distribuição de energia em um desses órgãos, poderia causar um prejuízo inimaginável.

Dos quesitos avaliados sobre senhas, backup, restrição ao acesso físico dos servidores centrais, controle de softwares instalados nas estações de trabalho do usuário, programa para identificação de invasões, vírus e spam, os índices foram bastante expressivos no sentido de que apontam para a adoção de boas práticas, por parte dos órgãos pesquisados.

- **A segurança dos sistemas de informação e o comportamento dos usuários.**

Pesquisa realizada por Pimenta e Quaresma (2016), teve como objetivo averiguar se o comportamento do usuário atua como mecanismo de proteção para

[5] http://www.cetic.br/tics/governo/2013/orgaos/B5/
[6] http://www.cetic.br/tics/governo/2015/orgaos/B6/expandido
[7] http://veja.abril.com.br/tecnologia/15-dos-orgaos-publicos-nao-tem-politica-de-seguranca-da-informacao/

a segurança dos sistemas internos ou como risco para uma organização. A verificação da pesquisa foi realizada através de um questionário online, que foi elaborado após um levantamento bibliográfico sobre a SI.

A área de atuação da pesquisa foi majoritariamente pessoas que trabalham em Portugal, sendo interrogado um total de 780 pessoas.

De acordo Pimenta e Quaresma (2016), os resultados gerados por esta pesquisa, levaram a concluir que os usuários praticam ações que, em sua maioria, atuam como mecanismos de proteção para a segurança dos sistemas internos. Ao final da análise, foi sugerido um conjunto de ações para que o usuário pudesse contribuir ainda mais com a segurança dos sistemas internos.

2.3 Considerações Finais do Capítulo

Neste capítulo foram descritos os conceitos que fundamentaram o estudo que avançou para a confirmação da hipótese levantada neste trabalho. Falou-se sobre o que é a informação; como ela é tratada na segurança da informação; o papel que o usuário desempenha na segurança da informação; algumas formas de ataque utilizadas para roubo de informação e formas de prevenção de possíveis ataques, fazendo uso de políticas dentro das organizações.

3. MATERIAIS E MÉTODOS

Neste capítulo será demonstrado como foi feito o procedimento de pesquisa adotado por este trabalho, que foi o levantamento de dados. A metodologia de pesquisa foi o método dedutivo, pois a análise foi feita a partir do geral, que foram casos de falhas nacionais para depois focar no particular, que foi a instituição. O tipo de pesquisa foi a pesquisa descritiva, cujo intuito foi descrever as características dos funcionários da UESB, envolvendo a aplicação de um questionário e posterior análise dos dados que foram coletados.

3.1 Metodologia

Considerando o objetivo principal deste trabalho, a população alvo deste estudo são os funcionários da UESB, Campus Vitória da Conquista, que para realizar as suas tarefas na instituição utilizam Sistema interno/Tecnologia da informação.

O universo de funcionários da UESB é diverso quanto a forma de admissão, sendo terceirizados, estagiários, servidores e provenientes do Regime Especial de Direito Administrativo (REDA), o que dificultou a contabilização. Para lidar com essa dificuldade de encontrar uma informação única do quadro de funcionários, foi feita uma estimativa usando os valores que foram fornecidos por cada setor responsável por uma forma de admissão diferente. Para essa pesquisa, trataremos nosso universo amostral o total de 500 funcionários.

A técnica de amostragem usada, foi probabilística. O instrumento escolhido para realizar a coleta de dados, foi um questionário. A coleta foi feita através do questionário impresso, entregue pessoalmente em cada setor da instituição, e online, através de link enviado por email para alguns setores que não haviam respondido ao questionário impresso, ficando disponível de 19 de abril a 13 de junho de 2017.

Os dados que foram obtidos com as respostas do questionário, foram objeto de uma pesquisa mista, quantitativa e qualitativa (sendo na sua maior parte quantitativa), posteriormente. Anteriormente à aplicação do questionário foi feita uma pesquisa bibliográfica acerca dos conceitos que seriam adotados no trabalho. Durante esta pesquisa, foi percebido alguns pontos chaves, em se tratando de falhas na segurança da informação por parte do usuário.

Em cima destes pontos, juntamente com a pesquisa de maturidade utilizada pelo Governo da Bahia citada na seção 2.2, foi elaborado o questionário de pesquisa.

O questionário (Apêndice 1) é composto por 15 questões, sendo 14 objetivas e uma objetiva com complementação subjetiva, e são divididas em grupos que se referem a pontos que implicam na SI. Estas questões abrangem procedimentos de segurança tendo o usuário como ator principal.

O primeiro grupo de questões, composto pela 1ª, 4ª e 5ª perguntas, teve como objetivo base saber se há uma normatização de boas práticas, ações preventivas e corretivas para manter a SI da instituição. Essas normas aparecem como um documento ou termo chamado de PSI.

O segundo grupo, formado pela 2ª e 3ª questões, tinha como objetivo, fazer um levantamento sobre os investimentos da instituição em treinamentos, campanhas de conscientização, se existem e se os usuários têm conhecimento deste processo.

A 6ª questão, aparece como terceiro grupo, composta de uma indagação objetiva e uma complementação subjetiva. Teve como ponto de análise, o correio eletrônico, fazendo um levantamento sobre se já houve alguma situação que colocasse em risco a SI, e como os usuários reagiram nessa situação.

O quarto grupo, composto da 7ª e 8ª perguntas, fez um levantamento a respeito do uso das senhas nos locais de trabalho. Se são senhas individuais, compartilhadas, ou se não fazem uso de senhas.

O quinto grupo, formado pela 9ª e 11ª questões analisou sobre a restrição de acesso ao conteúdo por parte de cada usuário e setor da instituição. Se a permissão de acesso ao conteúdo é dividida de acordo com o setor e cargo que cada usuário trabalha, ou se a permissão é igual para todos os funcionários.

A 10ª e 12ª perguntas, do sexto grupo, usaram como base o controle de entrada e saída de equipamentos e pessoal em cada setor da instituição, buscando averiguar se existe um registro de controle para possíveis eventualidades e comprovações.

O sétimo grupo, composto pela 13ª e 14ª indagações, analisou a utilização de dispositivos particulares no local do trabalho, considerando tanto dispositivos eletrônicos quanto dispositivos de armazenamento.

E o último grupo, composto pela 15ª questão, teve o objetivo de saber se há um feedback por parte dos usuários quanto à situação da SI na instituição, se há um índice de avaliação interno e se os usuários participam dessas avaliações.

A pesquisa obteve um total de 64 questionários respondidos, sendo todos válidos. O tamanho da amostra, inicialmente, foi calculado por técnica de amostragem probabilística.

Durante a aplicação dos questionários, houve uma grande resistência por parte dos usuários, quanto a disponibilidade de participar da pesquisa.

No decorrer das aplicações do questionário, foi percebida uma uniformidade nas respostas, o que possibilitou o fechamento da pesquisa por saturação teórica. “O fechamento amostral por saturação teórica é operacionalmente definido como a suspensão de inclusão de novos participantes quando os dados obtidos passam a apresentar, na avaliação do pesquisador, uma certa redundância ou repetição. ” (FONTANELLA et al, 2008)

3.1.1 Caracterização dos usuários pesquisados

Como o público alvo da pesquisa são os funcionários da UESB, Campus Vitória da Conquista, que usam um sistema interno/tecnologia da informação para execução de suas tarefas na instituição, existiram algumas diferenças em relação ao grau de instrução de um usuário pesquisado para o outro. Dentre os usuários pesquisados, foram abordados funcionários de cargos diversos que exigiam grau de escolaridade diferente. Sendo possível assim, identificar que foram entrevistados funcionários de grau de escolaridade superior e também funcionários com grau de escolaridade médio.

Como a identificação do usuário não era um item obrigatório no questionário, não há uma relação de quantos usuários de cada grau de escolaridade participaram.

3.2 Resultados e Discussão

Os resultados que serão mostrados a seguir são provenientes das respostas obtidas em cada grupo do questionário, cujo objetivo era encontrar ações que poderiam levar a possíveis falhas na SI.

- **Grupo 1: Política interna de Segurança da Informação**

Cerca de 89,1% dos respondentes dizem não ter assinado termo de confidencialidade quando assumiram o cargo na universidade (Figura 1). A não exigência da assinatura deste termo ao assumir o cargo, não cobra dos funcionários o comprometimento em respeitar as normas exigidas pela instituição e não os fazem assumir as consequências e punições de possíveis erros praticados pelos mesmos.

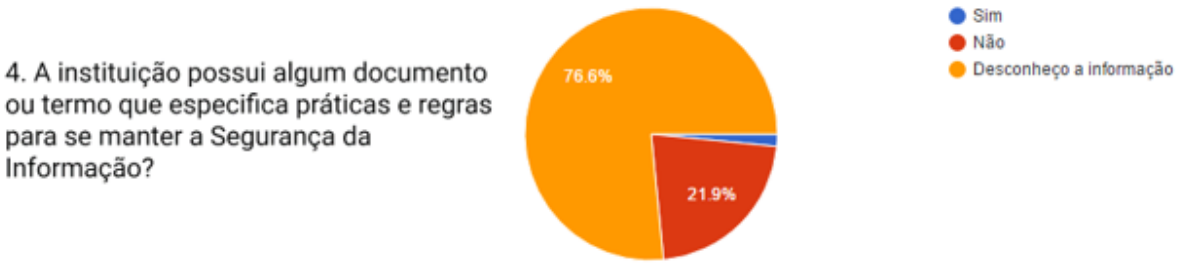
Figura 1: Resposta da questão sobre Termo de Confidencialidade

Fonte: Elaborada pela autora

O resultado dessa indagação leva a afirmar que a instituição não possui ou não faz uso de um termo de confidencialidade. A especificação de uso de um termo é inserida no conjunto de normas e práticas da SGSI interna, que é a PSI.

Em relação a existência de uma PSI na instituição, 76,6% dos respondentes afirmam desconhecer a informação sobre sua existência e 21,9% afirmam que não existem (Figura 2).

Figura 2: Resposta sobre a questão da PSI



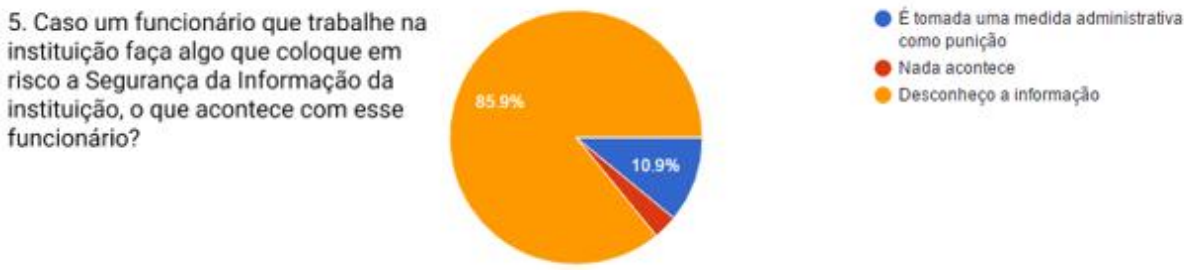
Fonte: Elaborada pela autora

A alta taxa de respostas afirmando o desconhecimento da informação sobre a existência de uma PSI, somada com a taxa de afirmações sobre a não existência da mesma, leva a afirmar que a instituição não divulga a PSI interna ou não possui uma PSI.

Como mostrado neste trabalho, a existência de uma PSI numa organização cria a cultura de conscientização sobre práticas que podem ajudar a reduzir falhas na SI. De acordo com Custódio (2015), é imprescindível a implantação de políticas de segurança no processo da organização de se proteger de ataques ou perdas de dados.

Em relação à consciência dos respondentes sobre as consequências da realização de práticas que coloquem em risco a SI da instituição, 85,9% dizem desconhecer as medidas punitivas, e somente 10,9% dizem saber de sua existência, e direciona como consequência, a tomada de uma medida administrativa (Figura 3).

Figura 3: Resposta da questão de consciência sobre as medidas punitivas



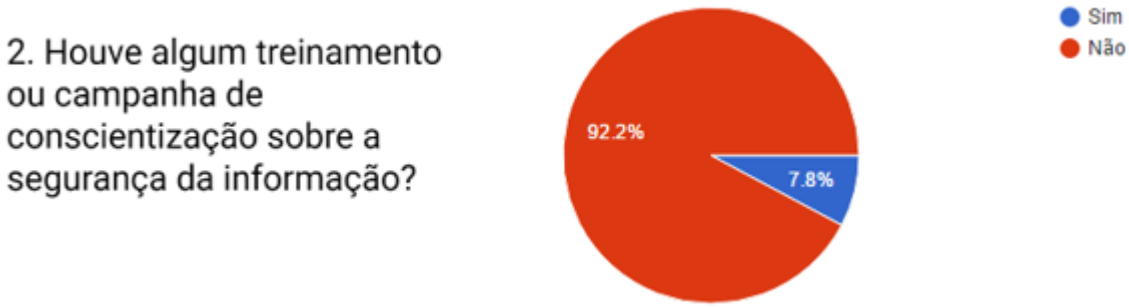
Fonte: Elaborada pela autora

A ausência de consciência sobre as consequências que surgem após algum ato que possa colocar em risco a SI da instituição, se deve à falta de um termo que descreva situações de risco e consequências se caso algumas ações não forem seguidas. Conforme dito por Fonseca (2009), para que exista essa consciência, a empresa deve criar e divulgar a PSI da instituição. Medidas punitivas contra ações erradas de funcionários, fazem com que os mesmos ponderem mais sobre suas ações.

- **Grupo 2: Treinamento**

Dos respondentes, 92,2% afirmam não ter participado de nenhum treinamento ou campanha de conscientização sobre a SI quando ingressaram na instituição (Figura 4), e quando perguntando sobre a frequência com que novos treinamentos são realizados, 75% afirmam que não existem treinamentos (Figura 5).

Figura 4: Resposta da questão sobre a oferta de treinamento



Fonte: Elaborada pela autora

A alta taxa indicando a não participação em treinamentos / campanhas de conscientização, leva a afirmar que os funcionários da universidade não são preparados ao assumirem suas funções na organização. Essa falta de instrução inicial, pode ser decorrente da não existência do treinamento ou da falta de divulgação do mesmo.

Figura 5: Resposta da questão sobre a frequência com que acontecem os treinamentos

Fonte: Elaborada pela autora

A reposta da questão 3, em sua maioria, levam a afirmar que a instituição não possui campanhas de conscientização / treinamento, o que pode ser um grande problema, pois os funcionários não são preparados para possíveis situações de risco ou falhas na SI.

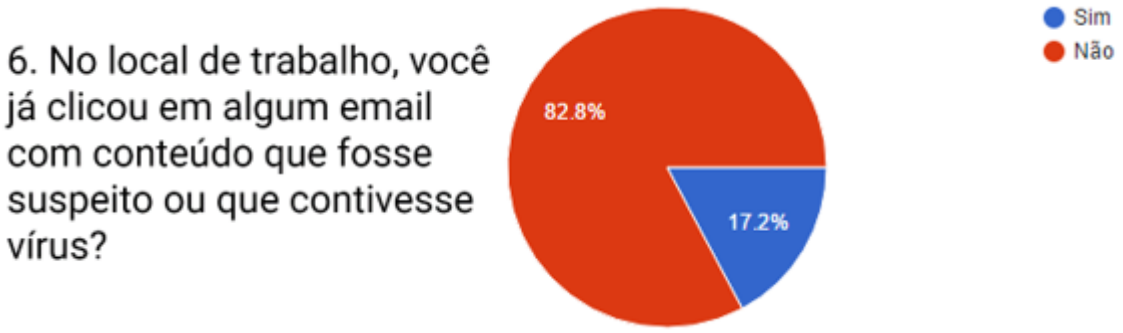
O treinamento cria no funcionário a consciência do seu papel no sistema de defesa da organização. Funcionários sob pressão, acabam por ignorar suas responsabilidades de segurança, portanto o treinamento deve ser muito mais que simplesmente impor regras (FONSECA, 2009). A falta de consciência e autoconfiança por parte dos colaboradores (a maioria das pessoas não se considera ingênua ou alvo fácil de ser ludibriada) fazem com que as investidas da ES sejam de sucesso.

Majoritariamente, as pessoas acreditam que os problemas ocasionados na SI são tratados somente pela parte tecnológica, como *firewall* e outras tecnologias afins, daí a importância da organização investir em treinamentos e campanhas de conscientização no âmbito da SI (ALVES, 2010).

- **Grupo 3: Correio eletrônico**

A respeito da consciência do usuário de não clicar em conteúdo de e-mails que sejam suspeitos, 82,8% afirmaram não clicar (Figura 6). Aqueles que afirmaram clicar nestes e-mails, descreveram através de uma questão aberta qual atitude foi tomada perante a situação de risco (Figura 7).

Figura 6: Resposta da questão sobre correio eletrônico

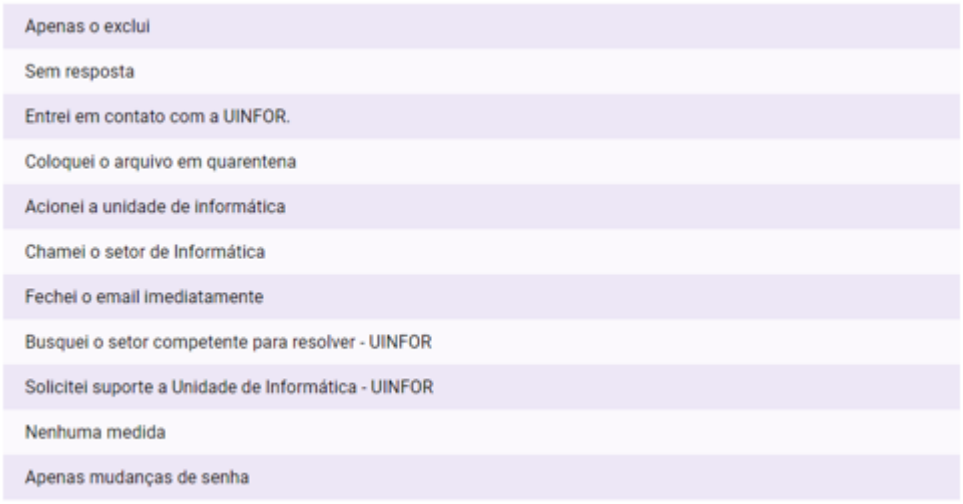


Fonte: Elaborada pela autora

A maioria dos respondentes mostrou ter certa preocupação e cuidado quanto ao uso do correio eletrônico no local de trabalho, o que pode diminuir substancialmente os riscos de caírem em ataques do tipo *spam*. Segundo Fontes

(2006 apud ROCHA, 2008), uma boa PSI precisa incluir melhores práticas para o uso do correio eletrônico afim de instruir os colaboradores de modo que não se tornem vítimas da ES, vírus ou armadilhas.

Figura 7: Resposta complementar sobre o Correio Eletrônico



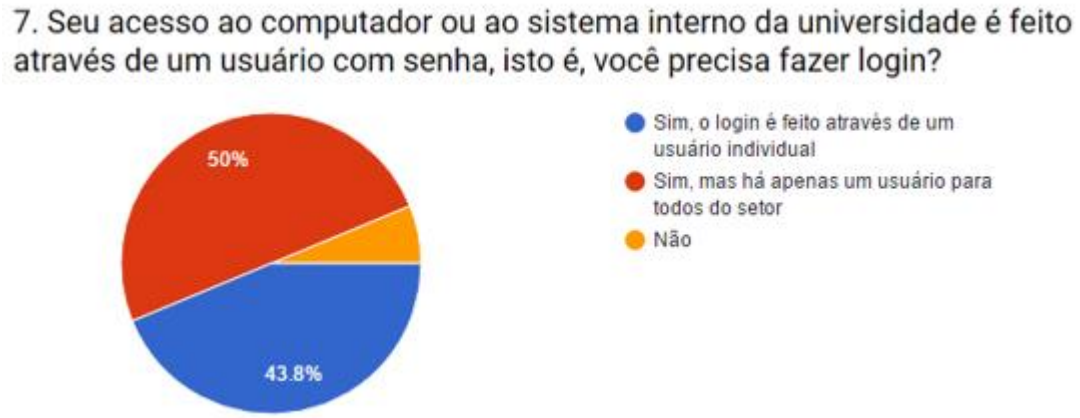
Fonte: Elaborada pela autora

Dos colaboradores pesquisados, 11 afirmaram ter clicado em e-mail contendo vírus ou conteúdo suspeito. Destes, 5 afirmaram reportar o problema ao setor competente da universidade, o setor de Informática. O restante tratou a situação como uma invasão por vírus comum, tentado soluções simples, ou não tomando medida alguma, o que oferece um grande risco para a instituição. Esta negligência deixa as informações presentes no computador, no sistema e na rede, vulneráveis.

- **Grupo 4: Senhas**

Quanto ao uso de senhas, houve uma divisão entre usar senhas por setor ou senhas individuais e não usar senhas (Figura 8). 50% dos respondentes afirmaram usar senhas de acesso que são compartilhadas por todos do setor, enquanto 43,8% afirmaram possuir senha de acesso individual.

Figura 8: Resposta da questão sobre o uso de senhas individuais



Fonte: Elaborada pela autora

O uso de senhas compartilhadas dificulta o controle dos acessos feitos pelos usuários. Senhas de acesso individuais permitem a identificação do que cada usuário fez no sistema/computador enquanto esteve conectado. Senhas compartilhadas ferem alguns princípios citados por Fontes (2006 apud Rocha, 2008), tais como a auditabilidade e não repúdio a autoria, ambos descritos na seção 2.2 desse trabalho.

Quando perguntando sobre a troca de senhas, 74,6% dos colaboradores afirmaram que não há exigência quanto a troca periódica de senha, e 23,8% disseram que a troca é feita quando o usuário desejar (Figura 9).

Figura 9: Respostas da questão sobre a troca períodica das senhas

Fonte: Elaborada pela autora

Conforme Mitnick (2005), as organizações que fazem uso de senhas estáticas, precisam oferecem treinamentos e lembretes ou campanhas de incentivos regulares para servir de incentivo a práticas seguras de senhas.

- **Grupo 5: Restrição de conteúdo**

Quando questionados sobre alterações no conteúdo a que tinha acesso, caso mudassem de cargos, 39,1% dos colaboradores disseram nunca ter mudado de cargo, portanto não poderiam opinar sobre esse aspecto. 39,1% afirmaram ter havido alteração de conteúdo quando mudaram de cargo, e 21,9% afirmaram não ter acontecido alteração quando mudaram de cargo (Figura 10).

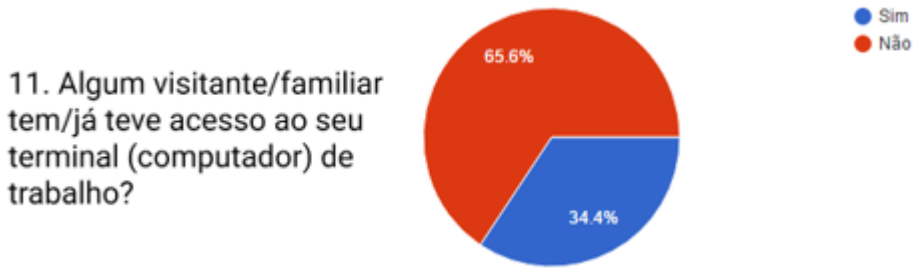
Figura 10: Resposta da questão sobre mudança de cargo

Fonte: Elaborada pela autora

Ainda que os quantitativos das repostas tenham sido valores bem próximos, a maior parte das mudanças de cargo foi precedida da alteração de conteúdo disponível, o que permite uma restrição maior no conteúdo de acesso e não ferindo o princípio da confidencialidade, apontado por Fontes (2006 apud ROCHA, 2008) e citado na seção 2.2 desta monografia.

Sobre a utilização do terminal de trabalho por parte de visitantes / familiares, 65,6% afirmaram não permitir esse acesso (Figura 11)

Figura 11: Resposta da questão sobre o uso do computador de trabalho por terceiros



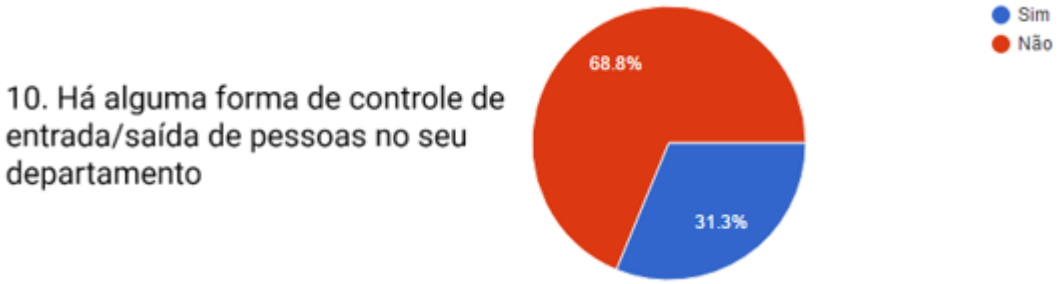
Fonte: Elaborada pela autora

A não utilização de computadores com conteúdo restrito por parte de terceiros dificulta o vazamento de informações indesejadas, contribuindo com a observação do princípio da confidencialidade mostrado na seção 2.2, visto que o engenheiro social usa de formas simples para conseguir roubar informações.

- **Grupo 6: Controle de entrada e saída de equipamentos e pessoas**

No quesito sobre registro de acesso de pessoas ao local de trabalho, 68,8% afirmaram que a entrada e saída de pessoas em seu setor é controlada (Figura 12).

Figura 12: Resposta da questão sobre controle de entrada e saída de pessoas

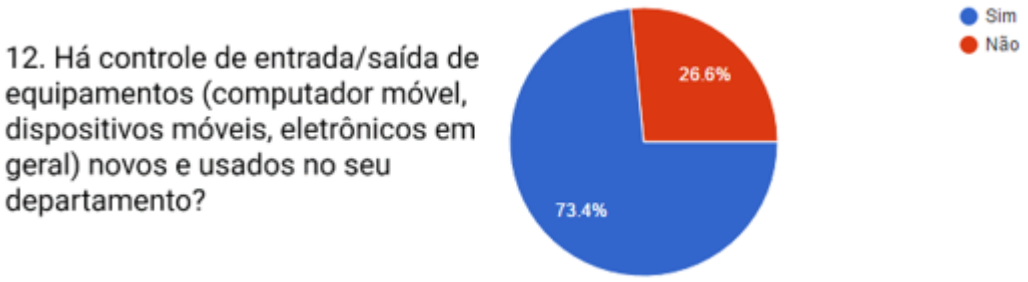


Fonte: Elaborada pela autora

Sem o controle de pessoas que transitam pelo setor, é inviável o reconhecimento de possíveis engenheiros sociais em ação – princípio de não repúdio de autoria, além de não ser possível identificar o nível de acesso que cada pessoa possui – princípio de confidencialidade, princípios citados na seção 2.2 deste trabalho.

Em relação a equipamentos (computador móvel, dispositivos móveis, eletrônicos em geral) novos e usados, 73,6% dos respondentes afirmaram que há registro de entrada e saída de tais equipamentos no setor (Figura 13).

Figura 13: Resposta da questão sobre o controle de entrada e saída de equipamentos



Fonte: Elaborada pela autora

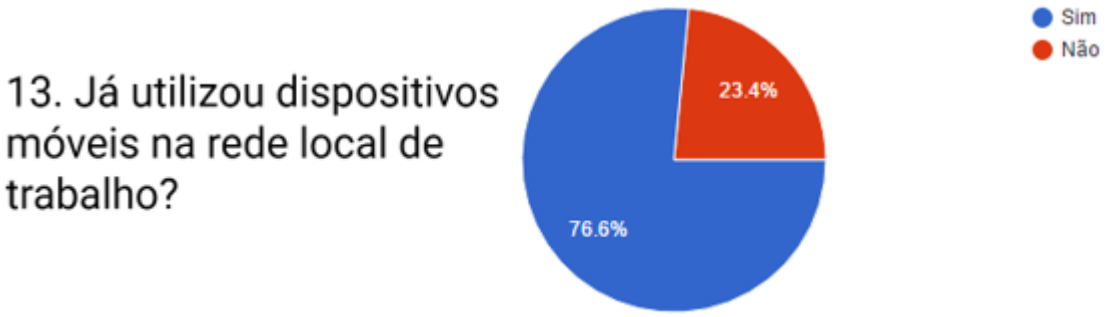
A maior parte dos respondentes afirmaram existir um controle de entrada e saída de equipamentos, induzindo à afirmação de que são menores as chances de acontecer falha na SI por equipamentos perdidos/roubados, como exemplo descrito na seção 2.3, em que as informações da organização foram vazadas através de ativos que foram roubados.

A segurança física dos ativos de tecnologia da informação é um aspecto primordial a ser projetado. Ao permitir acesso a locais restritos, funcionários mal-intencionados podem copiar dados sensíveis, sabotar servidores, equipamentos, e consequentemente causar resultados desastrosos para a instituição (BAHIA. Normas de Segurança da Informação, 2015). A inexistência deste controle nos setores tange os princípios da auditabilidade e não repúdio, descritos na seção 2.2.

- **Grupo 7: Dispositivos móveis particulares na rede local de trabalho**

Quando questionado aos funcionários sobre o uso de dispositivos pessoais no local de trabalho, 76,6 % afirmaram usar dispositivos móveis (celular, notebook) no local de trabalho (Figura14) e 65,6 % afirmaram usar dispositivos de armazenamento (pen drive, cartão de memória, HD externo) nos equipamentos de trabalho (Figura 15).

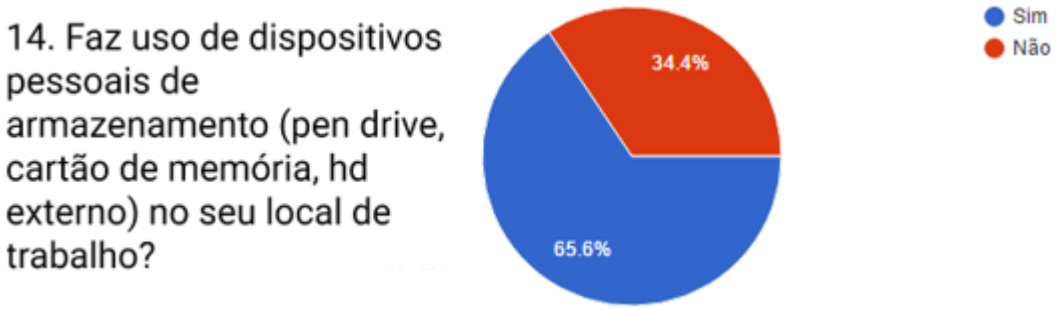
Figura 14: Resposta da questão sobre o uso de dispositivos móveis particulares na rede local



Fonte: Elaborada pela autora

A utilização de dispositivos móveis na rede do local de trabalho pode trazer alguns riscos, como facilitar o acesso a informações que estejam disponíveis apenas nessa rede. O fato da maioria dos respondentes afirmarem usar os dispositivos na rede local do trabalho demonstra que a conscientização do risco que ações como esta pode gerar, não existe.

Figura 15: Resposta da questão sobre uso de dispositivo de armazenamento no local de trabalho



Fonte: Elaborada pela autora

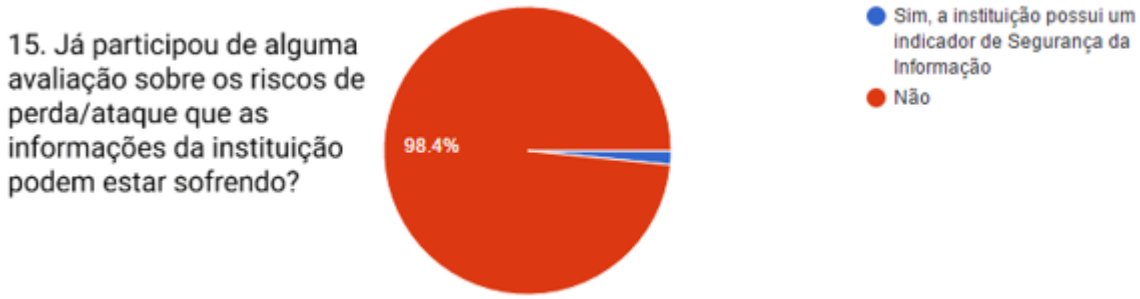
O uso de dispositivo de armazenamento pessoal para salvar informações de trabalho, pode ser um problema quando este dispositivo cai na mão de pessoas indesejadas, o que tange o princípio da auditabilidade. Além de representar um risco para a rede local se o dispositivo estiver carregando arquivo malicioso. Os colaboradores precisam estar sensibilizados quanto aos cuidados do uso de dispositivos de armazenamento particulares, conforme disseram Kruger e Kearney (2008 apud PIMENTA & QUARESMA, 2016).

A maior parte dos respondentes faz uso destes dispositivos pessoais no local de trabalho, o que leva a concluir que não há uma conscientização sobre os possíveis perigos desta ação.

- **Grupo 8: Índice de avaliação de perda / risco da Universidade**

Sobre a existência de um feedback por parte dos usuários, foi perguntado se os mesmos já haviam participado de alguma avaliação de riscos/perdas que a instituição tenha sofrido ou pudesse estar sofrendo. 98,4% dos respondentes afirmaram nunca ter participado dessa avaliação e desconhecem a informação deste índice de riscos.

Figura 16: Resposta da questão sobre a participação da avaliação de risco / perda da Universidade



Fonte: Elaborada pela autora

A quase unanimidade das respostas quanto ao quesito participação na avaliação de riscos, leva à conclusão de que não há um retorno avaliativo por parte dos usuários. Sem esta resposta é difícil ter uma noção do quanto a universidade está vulnerável.

3.3 Análise dos resultados

O questionário teve intuito de fazer um levantamento sobre as medidas de segurança que os funcionários da UESB praticam para manter a SI da instituição. De acordo às suas práticas, conclui-se que os colaboradores não estão preparados para exercer o seu papel dentro do SGSI.

Como resultado positivo, dentre as práticas realizadas pelos funcionários da instituição, pode-se destacar:

- Não abrem conteúdo de origem suspeita ou que contenha arquivo malicioso.
- Informam sobre incidentes com e-mails ao setor de informática responsável.
- As mudanças de cargo dentro da instituição foram sucedidas da respectiva alteração do acesso ao conteúdo específico para o cargo destinado.

- Não partilham seu computador com familiares ou visitantes do setor.
- Registram os equipamentos (computador e dispositivos móveis, eletrônicos em geral) que dão entrada e saída no seu setor.

Como resultados negativos, dentre as práticas realizadas pelos funcionários da instituição, destaca-se:

- Não assinam Termo de Confidencialidade, quando ingressam na instituição.
- Não participam de treinamento sobre SI.
- Não estão cientes sobre as consequências dos atos praticados.
- Compartilham senha de acesso aos sistemas inteligentes e computador de trabalho.
- Não realizam a troca periódica de senhas.
- Não registram a entrada e saída de pessoas nos seus setores.
- Utilizam dispositivos móveis particulares na rede local da instituição.
- Ligam dispositivos de armazenamento externo particular ao computador de trabalho.
- Não participam de avaliações sobre perdas/riscos que a instituição pode estar sofrendo.

Algumas das ações não praticadas pelos usuários, apontam na falha por parte da organização, destacando alguns fatores como:

- Ausência de campanhas de incentivos e treinamentos regulares.
- Ausência de documento ou termo que especifique as normas de SI da instituição, isto é, a PSI.

Não obrigatoriedade ou ausência de assinatura de Termo de Confidencialidade.

3.4 Considerações Finais

Neste capítulo foi feita a análise dos dados que foram obtidos através da aplicação do questionário de pesquisa, e avaliação das ações dos funcionários de acordo com as determinações da literatura estudada.

4. CONCLUSÃO

Este trabalho teve como objetivo analisar o conhecimento dos usuários da UESB quanto ao preparo para executar sua função dentro do SGSI da instituição, de modo que garantam a segurança da informação da instituição.

Os resultados analisados após aplicação do questionário de pesquisa, de uma forma geral, apontam para a falta de conhecimento dos usuários da UESB em exercer sua função dentro do SGSI. O fato de não exercerem práticas consideradas recomendáveis na literatura e que preservem a SI da instituição, demonstra que os usuários da UESB não estão preparados para exercer seu papel no processo de proteção dos ativos da informação da universidade.

No que se refere a possíveis melhorias a serem implantadas na SGSI da instituição, serão necessárias ações por parte do funcionário e por parte da organização. A começar pelas medidas que cabem à organização, apresenta-se procedimentos que irão aprimorar a SI da instituição:

- Gerar e divulgar um documento com a PSI interna, contendo práticas específicas ao nível crítico da informação com a qual cada setor da instituição lida.
- Exigir a utilização de senhas individuais, por colaborador.
- Exigir e estipularem um prazo de trocas periódicas de senhas.
- Bloquear a ligação de dispositivos de armazenamento externo em computadores da rede local.
- Criar campanhas de incentivos e treinamentos periódicos para sanar as possíveis dúvidas que os colaboradores venham a ter sobre a SI.
- Criar e aplicar o Termo de Confidencialidade ao processo de admissão dos colaboradores, discriminando as práticas devidas e consequências do não cumprimento das mesmas.
- Aplicar uma pesquisa interna para detectar os riscos e perdas que a instituição tenha sofrido, periodicamente.
- Fiscalizar a entrada e saída de pessoas em todos os setores da instituição.

A partir destas práticas implementadas pela organização, são pertinentes algumas ações a serem tomada pelos colaboradores da instituição, destacando-se

- Inteirar-se das normas e PSI da instituição, pois conhecendo o que é seu dever dentro da SGSI poderá aplicar as boas práticas na execução das suas atividades.
- Sempre que necessário, efetuar a troca de senhas e em momento algum, compartilhá-las. A troca periódica de senhas dificulta a ação por parte de algum cracker mal-intencionado.
- Ter cuidado ao utilizar dispositivos de armazenamento externo em computadores da rede local do trabalho, haja vista que não há como saber se o dispositivo está infectado com algum arquivo malicioso, o que pode representar um risco à SI.
- Reparar atentamente ao conteúdo dos e-mails que forem abertos no computador da rede local do trabalho. Arquivos maliciosos podem estar contidos em links disfarçados, e gerar um grande problema se não forem identificados antecipadamente por algum software de defesa
- Ter cuidado com o conteúdo que for acessado na internet dentro da rede local da instituição, ainda que esteja usando dispositivo particular
- Participar de treinamentos, campanhas de conscientização e avaliação de riscos da instituição. Estar consciente do seu papel na segurança dos dados da organização é a primeira grande medida que o usuário precisa tomar.

Durante o processo de estudo deste trabalho, houve dificuldades que restringiram, em parte, a atuação da pesquisa. As dificuldades surgiram na busca por trabalhos relacionados que pudessem embasar esta pesquisa, expondo uma escassez considerável no índice de trabalhos científicos na temática da SI no ponto de vista do usuário.

Para o cálculo do tamanho da amostra, notou-se a segunda dificuldade encontrada. A quantificação dos funcionários que trabalham na instituição, sob todas as formas de admissões existentes, não foi conseguida durante o período de realização da pesquisa. Entretanto, após o início das aplicações do questionário foi possível o fechamento por saturação teórica da pesquisa, o que tornou irrelevante o tamanho da amostra probabilística inicial.

4.1 Trabalhos futuros

Neste estudo foi alcançado o objetivo esperado, que era fazer uma análise sobre o preparo ou não dos funcionários da UESB em desempenhar o seu papel

dentro do SGSI da instituição, entretanto, por se tratar de uma área de extrema importância e com várias temáticas a serem pormenorizadas, fica a sugestão de trabalho a ser executado no futuro: a criação de uma PSI interna. A instituição não dispõe de uma PSI, o que aponta para a necessidade de um estudo que descreva as normas e características específicas necessárias para a proteção dos seus ativos da informação. A PSI descreve ações que são necessárias para o bom funcionamento da SI da organização.

Além disso, a criação de campanhas de treinamentos, para criar no usuário a consciência do que seus atos podem trazer para a proteção da informação da instituição e um guia de boas práticas a serem adotadas por todos os colaboradores da instituição.

REFERÊNCIAS

ABNT NBR ISO/IEC 27002:2005; **Tecnologia da Informação – Técnicas de Segurança** – Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005

ABNT NBR 6023:2002; **Informação e documentação - Referências – Elaboração.** Rio de Janeiro: ABNT, 2002.

ALVES, Cassio B.; **Segurança da Informação vs. Engenharia Social.** Como se proteger para não ser mais uma vítima. Brasília, 2010. 63 f. Disponível em http://www.administradores.com.br/_assets/modules/academicos/academico_3641.pdf. Acessado em 04 de abril de 2017.

CAPURRO, Rafael e HJORLAND, Birger.; **O conceito de informação**. Capítulo traduzido publicado no Annual Review of Information Science and Technology. Ed. Blaise Cronin. v. 37, cap 8, p 343 – 411.

CUSTÓDIO, Paulo V. da C.; **Políticas de Segurança da Informação e tendências de mercado para Organizações de TI**. Palhoça, UNISUL, 2015. Monografia (Especialização) - Gestão de Segurança da Informação, Universidade do Sul de Santa Catarina.

FONSECA, Paula F.; **Gestão de Segurança da Informação:** O Fator Humano. 2009. 16 f. Monografia (Especialização) – Redes e Segurança de Computadores, Pontifícia Universidade Católica do Paraná, Curitiba, 2009. Disponível em: <http://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/Paula%20Fernanda%20Fonseca%20-%20Artigo.pdf>. Acessado em 04 de abril de 2017.

FONTANELLA, Bruno J. B.; RICAS, Janete; TURATO, Egberto R.; **Amostragem por saturação em pesquisas qualitativas em saúde: contribuições teóricas.** Rio de Janeiro, 2008. Disponível em < http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0102-311X2008000100003>. Acessado em 26 de julho de 2017.

FONTES, Edison; **Segurança da Informação**: o usuário faz a diferença. 1a edição. São Paulo: Saraiva, 2006.

GAIER, Rodrigo V.; SAVARESE, Maurício; **Roubo de dados da Petrobrás foi espionagem, diz PF**. Reuters/Brasil Online, Rio de Janeiro, 19 de fevereiro. 2008. Disponível em: <https://oglobo.globo.com/economia/roubo-de-dados-da-petrobras-foi-espionagem-diz-pf-3632874. Acessado em 01 de abril de 2017.

MARTINS, Elaine; **Cuidado com a engenharia social**. 2008. Disponível em <ttps://www.tecmundo.com.br/msn-messenger/1078-cuidado-com-a-engenharia-social.htm?utm_source=404corrigido&utm_medium=baixaki>. Acessado em 04 de abril de 2017.

MESSIAS, Lucilene C. da S.; **Informação: um estudo exploratório do conceito em periódicos científicos brasileiros da área de Ciência da Informação**. Marília, UNESP, 2005, 206 f. Tese (Mestrado em Ciência da Informação) – Programa de Pós-Graduação em Ciência da Informação, da Universidade Estadual Paulista – UNESP (Área de Concentração: Informação, Tecnologia e Conhecimento), 2005.

MITNICK, Kevin D.; SIMON, William L. **A arte de invadir:** as verdadeiras histórias por trás das ações de hackers, intrusos e criminosos eletrônicos. São Paulo: Pearson Prentice Hall, 2005.

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar:** Ataque de hackers: controlando o fator humano na Segurança da Informação. São Paulo: Pearson Prentice Hall, 2003.

PEIXOTO, Mário C. P.; **Engenharia Social e Segurança da Informação na Gestão Corporativa**. Rio de Janeiro: Brasport, 2006

PIMENTA, Alexandre M. S.; QUARESMA, Rui F.C.; **A Segurança dos sistemas de informação e o comportamento dos usuários.** Journal of Information Systems and Technology Management, São Paulo, p 533-552, dez de 2016.

ROCHA, Paulo C. C.; **Segurança da Informação** – Uma questão não apenas tecnológica. 2008, 61 f. Monografia (Especialização) - Gestão da Segurança da Informação e Comunicações, Universidade de Brasília Instituto de Ciências Exatas Departamento de Ciência da Computação, 2008. Disponível em: <http://dsic.planalto.gov.br/documentos/cegsic/monografias_1_turma/paulo_cesar.pdf>. Acessado em 26 de março de 2017.

SILVA FILHO, Antonio M.da; **Segurança da Informação**: Sobre a Necessidade de Proteção de Sistemas de Informações. 2008. Disponível em: <http://www.espacoacademico.com.br/042/42amsf.htm>. Acessado em 20 de março de 2017.

APÊNDICE 1 – QUESTIONÁRIO DA PESQUISA

Questionário para elaboração de uma pesquisa para o trabalho de conclusão do curso de Ciência da Computação pela Universidade Estadual do Sudoeste da Bahia.

Identificação

Nome: _____

Cargo: _____Setor: _____

1. **Quando ingressou na instituição, assinou algum termo se comprometendo a manter as informações referentes ao seu trabalho em confidência?**
   a. SIM( ).
   b. NÃO( ).
2. **Houve algum treinamento ou campanha de conscientização sobre a segurança da informação? Entenda como segurança da informação, todas as ações necessárias para manter os dados da instituição seguros, como: formas de acesso aos computadores e internet; definição do nível de segurança exigido para o tipo de informação que seu setor trata; forma de acesso a e-mails.**
   a. SIM( )
   b. NÃO( ).
3. **Com que frequência são ministrados novos treinamentos ou campanhas de conscientização referentes à Segurança da Informação?**
   a. Bimestral ( ).
   b. Trimestral ( ).
   c. Semestral ( ).
   d. Anual ( ).
   e. Não há um período fixo, mas os treinamentos/campanhas acontecem( ).
   f. Não há treinamento( ).
4. **A instituição possui algum documento ou termo que especifica práticas e regras para se manter a Segurança da Informação?**
   a. NÃO( ).
   b. SIM( ).
   c. Desconheço a informação( ).
5. **Caso um funcionário que trabalhe na instituição faça algo que coloque em risco a Segurança da Informação da instituição, o que acontece com esse funcionário?**

a. É tomada uma medida administrativa como punição( ).

b. Nada acontece( ).

c. Desconheço a informação( ).

6. No local de trabalho, você já clicou em algum email com conteúdo que fosse suspeito ou que contivesse vírus?

a. SIM( ).

b. NÃO( ).

Se a resposta do quesito anterior foi SIM, qual medida você tomou?

_____
_____
_____

7. Seu acesso ao computador ou ao sistema interno da universidade é feito através de um usuário com senha, isto é, você precisa fazer login?

a. SIM( ).

b. NÃO( ).

8. Com que frequência é feita a troca da senha do usuário?

a. Não há exigência de troca periódica de senha( ).

b. A troca é feita no período que o usuário desejar( ).

c. A troca é feita obrigatoriamente no período de _____.

9. Já mudou de cargo/setor de quando ingressou no trabalho? Quando mudou de cargo/setor, houve alteração no conteúdo a que tinha acesso?

a. Nunca mudou de cargo/setor( ).

b. Mudou de cargo/setor mas não houve alteração no acesso à informação( ).

c. Mudou de cargo/setor e houve alteração no acesso à determinadas informações( ).

10. Há alguma forma de controle de entrada/saída de pessoas no seu departamento?

a. SIM( )

b. NÃO( )

11. Algum visitante/familiar tem/já teve acesso ao seu terminal (computador) de trabalho?

a. SIM( ).

b. NÃO( ).

12. Há controle de entrada/saída de equipamentos (computador móvel, dispositivos móveis, eletrônicos em geral) novos e usados no seu departamento?

a. SIM( ).

b. NÃO( ).

13. Já utilizou dispositivos móveis na rede local de trabalho?

a. SIM( ).

b. NÃO( ).

14. Faz uso de dispositivos pessoais de armazenamento (pen drive, cartão de memória, hd externo) no seu local de trabalho?

a. NÃO( ).

b. SIM( ).

15. Já participou de alguma avaliação sobre os riscos de perda/ataque que as informações da instituição podem estar sofrendo?

a. NÃO( ).

b. SIM, a instituição possui um indicador de Segurança da Informação( )

ANEXO 2 – PESQUISA DE MATURIDADE APLICADA PELO ESTADO DA BAHIA

PROPOSTA PARA PESQUISA DE MATURIDADE 2015 / 2016

1. **Quantos usuários de rede ativos possui a sua Organização? (Questão 2)**
   de 1 a 100 usuários
   de 101 a 500 usuários
   de 501 a 1000 usuários
   de 1001 a 2000 usuários
   Acima de 2000 usuários

2. **Com relação à implantação das normas de Segurança da Informação, como se encontra a situação da sua organização?**
   Não implementada-Implementadaparcialmente-Implementada
   Norma 1
   Norma 2
   Norma 3
   ...

3. **Selecione a(s) solução(es) que a sua organização possui.Escolha a(s) que mais se adequa(m).**
   Firewall (não é o da PRODEB)
   UTM
   VLAN
   Filtro WEB
   IPS
   Antivírus corporativo

4. **Sua Organização possui orçamento para Segurança da Informação?**
   Sim
   Não

5. **Sua organização possui um profissional responsável pela segurança da informação?**
   Não
   Sim, um profissional da área de TI
   Sim, um profissional específico de segurança da informação

6. **Algum treinamento ou campanha de conscientização sobre segurança da informação foi promovido pela sua Organização no último ano?**
   Não
   Sim, apenas 01 vez

Sim, mais de 01 vez

7. **Os usuários da sua organização assinam Termo de Sigilo e Confidencialidade?**
   Sim
   Não

8. **O acesso remoto a rede corporativa ou Intranet é feito através de um canal de acesso seguro (VPN - Virtual Private Network ou outro recurso semelhante)?**
   Não é feito acesso remoto
   Não é utilizado um canal seguro
   É utilizado um canal seguro

9. **Sua organização possui rotina formal de backup das informações?**
   Não
   Sim, mas não é realizado teste de restore
   Sim, com a realização de teste de restore

10. **Como são armazenadas as fitas de backup com conteúdo sigiloso? Escolha a(s) que mais se adeque(m).**
    Em um armário ou similar
    Em um cofre comum
    Em um cofre anti-chamas
    Em ambiente off-site

11. **Sua organização possui rede sem fio?**
    Não
    Sim, com controladora de rede sem fio
    Sim, sem controladora de rede sem fio

12. **Sua organização possui um procedimento formal para concessão e revogação de acesso aos recursos de TI?**
    Sim / Não

13. **Sua política de gestão de senhas contempla (marque todas as alternativas utilizadas em sua organização):**
    Não há uma política de gestão de senhas.
    Regras para criação de senhas seguras
    Obrigatoriedade de troca da senha inicial

Obrigatoriedade de troca periódica de senha
Revogação de senha em caso de desligamento
Bloqueio de senha em caso de afastamento temporário (férias, licenças, etc)

14. **Sua organização possui um procedimento de concessão e revogação de direitos de acesso à rede e sistemas?**
    Não
    Sim, porém não existe uma revisão periódica dos direitos de acesso
    Sim, com revisão periódica dos direitos de acesso

15. **Sua Organização mantém quais registros (logs)? Escolha a(s) que mais se adeque(m).**
    Não há armazenamento dos registros
    Log de acesso à rede
    Log de acesso às aplicações
    Log de acesso à Internet

16. **Existe um procedimento para o registro e a notificação dos incidentes de Segurança da Informação?**
    Não
    Sim, através de processo manual
    Sim, através de ferramenta informatizada

17. **Existe um procedimento para o tratamento dos incidentes de Segurança da Informação?**
    Sim / Não

18. **Sua Organização realiza auditorias de Segurança da Informação?**
    Sim / Não

19. **Sua organização possui algum indicador de Segurança da Informação?**
    Sim, com base nestes indicadores são feitas melhorias contínuas
    Sim
    Não

    Qual(is) ? (a pergunta é dependente da anterior e não está numerada)
    Campo texto para que seja informado

20. **Dentre as iniciativas de Gestão de Continuidade de Negócios, marque os planos que estão implementados em sua organização. Escolha a(s) que mais se adeque(m).**
    Nenhuma iniciativa
    Plano de Continuidade Operacional (PCO)
    Plano de Recuperação de Desastre (PRD)
    Plano de Administração de Crise (PAC)

21. **O(s) Plano(s) que integra(m) a Gestão de Continuidade de Negócios da sua organização são submetidos à revisão e teste?**
    Sim
    Não

22. **Sua organização realiza Gestão de Riscos?**
    Não
    Sim, existe um processo informal
    Sim, existe um processo formal e utiliza uma ferramenta informatizada
    Sim, existe um processo formal

23. **O ambiente que abriga os servidores, equipamentos de armazenamento de dados e ativos de rede da sua Organização é protegido contra acesso físico não autorizado?**
    É utilizada a sala cofre da PRODEB.
    Sim
    Não

24. **Os Ativos de Tecnologia da Informação críticos são protegidos por equipamentos contra falhas de energia e outras anomalias na alimentação elétrica?**
    Sim / Não

25. **Sua organização utiliza ferramentas de software homologadas pela área de Tecnologia da Informação?**
    Não
    Sim, todas
    Sim, mas nem todas

26. **Sua organização utiliza ferramentas de software licenciadas?**
    Não
    Sim, todas
    Sim, mas nem todas

27. **Em sua organização o ambiente de desenvolvimento e teste são isolados do ambiente de homologação e produção?**
    Não há desenvolvimento
    Desenvolvimento
    Homologação
    Produção

28. **No envio de equipamentos para manutenção externa:**
    Utilizamos o procedimento de cópias de segurança (backup) e descarte seguro das informações em mídias eletrônicas
    Não utilizamos os procedimentos de cópias de segurança (backup) e descarte seguro das informações em mídias eletrônicas

29. **Sua Organização possui algum processo de gerenciamento de mudança?**
    Não
    Sim, existe processo informal
    Sim, existe processo formal e, com base em indicadores, são feitas melhorias contínuas
    Sim, existe processo formal, porém sem avaliação de indicadores