CIÊNCIASGERENCIAIS em foco

ISSN: 2317-5265 – v. 9, n. 6 (2018) - UEMG - CLÁUDIO

ANÁLISE DA PERCEPÇÃO DE SEGURANÇA DA INFORMAÇÃO DE UMA COOPERATIVA DE CRÉDITO DO CENTRO OESTE/MG POR PARTE DE SEUS COLABORADORES

Isabel Alice Resende de Azevedo[1]
Sabrina Vieira de Melo[2]
Humberto Gomes Pereira[3]
José Marcelo Fraga Rios[5]

RESUMO

A segurança da informação é uma questão primordial quando se trata de tecnologia tanto na vida pessoal quanto no cotidiano em organizações, e tem como objetivo evitar fraudes como vazamentos e perda de informações. O presente estudo busca, através de uma pesquisa qualitativa, definir os conceitos de segurança da informação, a sua importância para as organizações bem como analisar através da participação dos funcionários e demais associados de uma cooperativa de crédito o se grau de conhecimento da política da segurança da informação e suas atitudes como forma de sua proteção. Perante os resultados obtidos nesta pesquisa, destacamos a existência de uma política de segurança da informação na organização, porém, não conhecida pela totalidade de seus colaboradores. Buscamos, ainda, analisar a forma com que os colaboradores utilizam as estações de trabalho.

Palavras-chave: segurança da informação, politica da segurança da informação, fraudes.

ABSTRACT

The Information security is a key issue when it comes to technology, both in personal life and daily life in organizations, with the aim of avoid frauds such as leaks and loss of information. The present study searches through a qualitative research, definer the concepts of information security, the information security's importance as well as to analyze through the participation of employees and other members of a credit union the degree of knowledge about the information security policy and employee's actions as a way of protecting yourself. Considering the results obtained in this research, highlight the existence of an information security

[1]Professor e orientador – FACED – rafahdiniz@yahoo.com.br
[2]Pós-graduanda em Gestão Contábil, Auditoria e Controladoria pela FACED - isabelazevedoadm@gmail.com
[3]Pós-graduanda em Gestão Contábil, Auditoria e Controladoria pela FACED - sabrinamelov@hotmail.com
[4] Professor e orientador – FACED – humberto.pereira@uemg.br
[5]Pós-graduando em Gestão Contábil, Auditoria e Controladoria pela FACED – mfragarios@gmail.com

ISSN: 2317-5265 – v. 9, n. 6 (2018) - UEMG - CLÁUDIO

policy in the organization, but this information security policy is not known by all of its employees. We will analyses how the employees use their workstations.

Keywords: information security, information security policy, fraud.

INTRODUÇÃO

Com a constante evolução da tecnologia, as empresas passaram a utilizar cada vez mais os sistemas de informação no processamento de várias tarefas. Uma dessas tarefas é a confecção de cadastro de clientes e sua análise econômica financeira em uma cooperativa de crédito.

Neste estudo, abordaremos a percepção da segurança da informação no sistema utilizado por funcionários de uma cooperativa de crédito do Centro Oeste de Minas Gerais. A pesquisa foi realizada na Cooperativa Sicoob Divicred. O Sicoob Divicred é uma instituição financeira cooperativa fundada em 8 de maio, de 1997 autorizada pelo Banco Central do Brasil e filiada ao Sicoob Central Cecremge. Com o intuito de fornecer recursos a sociedade, promove o crescimento social e econômico, uma vez que aplica na própria região de atuação a maior parte dos recursos captados na busca do que é mais lucrativo para seus associados.

Como princípio básico do cooperativismo o Sicoob Divicred é uma instituição sem fins lucrativos com foco na cooperação e concessão de boas condições financeiras de forma desburocratizada. No cooperativismo os associados também são donos do negócio, por isso, as sobras financeiras ou lucro como é denominado nos bancos convencionais, são distribuídas anualmente aos associados.

Embasado em um planejamento sério, transparente e dinâmico afirma um só propósito – oferecer confiabilidade, facilidade e atendimento direcionado às necessidades de cada cooperado com condições personalizadas valorizando a união, cooperação, ética, profissionalismo, inovação e o relacionamento com os mais de 11 mil cooperados.

Hoje o Sicoob Divicred atende em nove pontos de atendimento distribuídos no centro-oeste e região metropolitana de Minas Gerais sendo quatro Postos de Atendimento em Divinópolis, um em Carmo do Cajuru, um em Belo Horizonte, um em Betim e um em Contagem.

ISSN: 2317-5265 – v. 9, n. 6 (2018) - UEMG - CLÁUDIO

Ao fazer uma consulta interna nos dados cadastrais para realizar o levantamento da situação econômica e financeira das empresas que mantém negócios na Cooperativa, alguns procedimentos devem ser seguidos pelos responsáveis por essa atividade dentro da empresa. A segurança das informações é de suma importância para qualquer empresa e extremamente vital em uma empresa que têm por finalidade o apoio no desenvolvimento e liberação de crédito para os seus clientes.

Percebe-se que a empresa que utiliza a plataforma da segurança da informação é vista de forma diferenciada pelos seus clientes e funcionários e estará protegida por ações contínua de fraudes, invasão em redes e evitando assim, que suas estações de trabalho não sejam corrompidas e infectadas por vírus e ataques cibernéticos.

Sabendo que as empresas necessitam de proteção e devem criar filtros que impeçam o uso dessas informações de forma indevida, questiona-se: a segurança dessas informações estão seguras de ataques cibernéticos e de quebra de sigilo na empresa estudada? Os funcionários da Cooperativa utilizam o sistema de forma a evitar a contaminação por vírus e ataques cibernéticos e proteger os dados utilizados?

Para responder aos questionamentos, apresenta-se uma entrevista envolvendo 14 (quatorze) pessoas, onde analisaremos o conhecimento e utilização da segurança da informação na cooperativa, sua forma de utilizar as estações de trabalho e a conscientização dos funcionários envolvidos na utilização dos dados sobre o valor da informação para os negócios.

METODOLOGIA

A pesquisa desenvolvida foi baseada no método quantitativo, que segundo Prodanov e Freitas (2013), considera que tudo pode ser quantificável, o que significa traduzir em números, as opiniões e informações para classificá-las e analisá-las. Ela requer o uso de recursos e de técnicas estatísticas como percentagem, média,

ISSN: 2317-5265 – v. 9, n. 6 (2018) - UEMG - CLÁUDIO

moda, mediana, desvio padrão, coeficiente de correlação, análise de regressão, dentre outros.

Em relação aos procedimentos técnicos para a coleta de dados, a pesquisa utilizou-se da pesquisa bibliográfica e de entrevistas com os funcionários sobre o cenário de segurança da informação na empresa alvo mediante questionário *online* enviado para os funcionários da cooperativa de crédito. O questionário dispõe de dez questões entre múltipla escolha e abertas.

RESULTADOS E DISCUSSÃO

CONCEITOS DE SEGURANÇA DA INFORMAÇÃO

Definições

A Segurança da Informação tem ganhado destaque nos últimos anos devido ao seu valor tanto para usuários quanto para empresas. A segurança envolve medidas responsáveis em proteger contra atos como espionagens, roubos, ataques cibernéticos e golpes dentre outras práticas.

A segurança resulta na condição de seguro e adequadamente protegido em situações perigosas. Segundo Sêmola (2003), a informação é "algo que se conhece e em que se baseia para racionalizar". Na comunicação dos seres humanos a informação é essencial para sobrevivência e convívio entre si. Ainda conforme Sêmola (2003, p.45), define a informação como:

> Conjunto de dados utilizados para transferências de uma mensagem entre indivíduos e/ou máquinas em processos comunicativos, isto é, baseados em trocas de mensagens ou transacionais, e processos em que sejam realizadas operações que envolvem, por exemplo, a transferências de valores monetários (SÊMOLA, 2003, p. 45).

A Segurança da Informação consiste no conjunto dos significados citados acima, ou seja, proteção ao conjunto de informações sejam eles de uma empresa, pessoais para que não sejam copiados, alterados e consultados por indivíduos não autorizados. Continuando, Sêmola (2003, p.45) explica segurança da informação

ISSN: 2317-5265 – v. 9, n. 6 (2018) - UEMG - CLÁUDIO

como um campo do conhecimento dedicado à proteção da informação contra acessos não permitidos, alterações indevidas ou sua indisponibilidade.

Para a Norma Regulamentadora (NBR) *International Organization for Standardization* (ISO) *International Electrotechnical Commission* (IEC) denominada ISO/IEC 27002 da Associação Brasileira de Normas Técnicas (ABNT, 2013), a segurança da informação "é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware".

A norma define itens como: Escopo, Referências normativas, Termos e definições, Estrutura da Norma, Políticas de segurança da informação, Organização da segurança da informação, Segurança em recursos humanos, Gestão de ativos, Controle de acesso, Criptografia, Segurança física e do ambiente, Segurança nas operações, Segurança nas comunicações, Aquisição, desenvolvimento e manutenção de sistemas, Relacionamento na cadeia de suprimento, Gestão de Incidentes de Segurança da Informação, Aspectos da segurança da informação na gestão da continuidade do negócio, e, Conformidade.

Recomenda-se que as empresas utilizem os princípios da certificação NBR ISSO/IEC 27002 (ABNT, 2013) e trabalhem com profissionais qualificados e certificados por essa norma para auxílio na implantação dos controles relacionados.

Importância da Segurança da Informação

O tema Segurança da Informação vem se tornando assunto cotidiano nas grandes mídias devido a sua evolução e, em muitas vezes, relacionado aos danos causados em cenários de perda ou roubo de dados.

A Tecnologia da Informação tem evoluído a passos largos fazendo com que as organizações sejam eficientes e ágeis na tomada de decisões, e atualmente, as chances de uma empresa não utilizar sistema de segurança da informação é praticamente nula visto que o contexto atual é marcado e representado por ações contínuas de fraudes, invasões em redes e estações de trabalho captando informações sigilosas das empresas, colocando em questão a fragilidade e

ISSN: 2317-5265 – v. 9, n. 6 (2018) - UEMG - CLÁUDIO

desconhecimento de todos que utilizam as redes de acesso de uma determinada organização.

Garantir níveis de proteção para as informações é essencial, pois deve-se sempre observar os prejuízos impostos com a perda de dados. Segundo Fonseca (2009, p. 51), “é através do fator humano que ocorre grande parte dos vazamentos de informações, seja por descontentamento do colaborador com a organização, o qual pode não se sentir valorizado ou por técnicas de Engenharia Social”.

Percebe-se a senso comum que, na maioria das vezes, é evidenciado o mau uso das ferramentas de trabalho, onde o colaborador utiliza o terminal de trabalho com fins de utilização pessoal, comprometendo informações das organizações e expondo ela a riscos incalculáveis.

Uma forma das organizações se protegerem é através da implantação de Políticas de Segurança da Informação, visando minimizar eventuais riscos por quebra de confiabilidade, integralidade e disponibilidade das informações das empresas. Ela procura adotar diversos mecanismos para proteção de dados. A política de segurança funciona como um conjunto de procedimentos que direciona os funcionários para agir de forma que ela imponha a eles procedimentos para evitar os danos causados pela perda nas informações.

Conforme Campos (2007), a ameaça pode ser considerada um agente externo ao ativo de informação, pois se aproveita de suas vulnerabilidades para quebrar a os princípios básicos da informação como a confidencialidade, a integridade ou disponibilidade.

SEGURANÇA DA INFORMAÇÃO NAS ORGANIZAÇÕES

FORMAS DE PROTEÇÃO DAS INFORMAÇÕES

Atualmente existem inúmeros mecanismos de proteção para as informações, tanto pessoais quanto empresariais. Essas proteções têm por objetivo proteger os dados dos usuários e organizações que tanto dependem de seus ativos tecnológicos.

ISSN: 2317-5265 – v. 9, n. 6 (2018) - UEMG - CLÁUDIO

A segurança da informação envolve dois aspectos distintos, o físico e o lógico. Para Pinheiro (2009), a segurança física tem por objetivo a proteção de equipamentos contra usuários não autorizados, caracterizando-se pela segurança de perímetros e instalações. O autor ressalta que para a proteção física são recomendados alguns artifícios como o controle de entrada e saída de materiais, equipamentos, pessoal, registro de data e horários, bem como os responsáveis pelos mesmos.

Vale ressaltar que a segurança da informação deve ser iniciada pela parte física para o lógico, pois de nada adianta investir muito dinheiro em sistemas sofisticados e softwares robustos, se o invasor consegue o acesso fisicamente ao dispositivo tecnológico.

Conforme Pinheiro (2009, p.15), a segurança lógica tem a preocupação em "proteger os dados, programas e sistemas contra tentativas de acessos não autorizados, feitas por usuários ou outros programas". O autor ainda apresenta (2009, p.15), os recursos e informações que devem ser protegidos: "Aplicativos (Programas fonte e objeto); Arquivos de dados; Utilitários e Sistema operacional; Arquivos de senha; e, Arquivos de log."

Os controles lógicos procuram limitar e impedir o acesso as informações e estão em ambiente controlado por meio eletrônico e restrito aos não autorizados para não ficar exposto correndo o risco de sofrer alterações. Pinheiro (2009) diz que alguns dos mecanismos de proteção são listados a seguir:

- Mecanismos de criptografia: é uma técnica de linguagem transformada em sua forma original para ser reconhecida apenas pelo destinatário o que dificulta a leitura para não autorizados
- Assinatura digital: é uma forma de autenticação de documentos por meio digital substituindo a assinatura física eliminando o documento em papel.
- Controle de acessos: uso de palavra chaves, cartões inteligentes, sistema biométrico, firewalls e senhas.

ISSN: 2317-5265 – v. 9, n. 6 (2018) - UEMG - CLÁUDIO

Existem atualmente vários sistemas e empresas que buscam fornecer proteções para esses ambientes, como os antivírus com a capacidade de detectar invasões e impedir o acesso dos vírus ao banco de dados e à rede de acesso aos dados.

Disponibilidade, integridade e confidencialidade

Ter na empresa a Segurança da Informação significa garantir que as informações existentes em qualquer formato estejam seguras contra o acesso por pessoas não autorizadas tornando confidencial essas informações e acessadas somente por pessoas autorizadas, que esteja sempre à disposição quando necessária para consultas e verificação, confiável e autêntica e que não possa ser manipulada indivíduo não autorizado.

Segundo Fontes (2006, p.20), proteger a informação significa garantir:

> 1.Disponibilidade: a informação deve estar acessível para o funcionamento da organização.
> 2.Integridade: a informação deve estar correta, ser verdadeira e não estar corrompida.
> 3.Confidencialidade: a informação deve ser acessada exclusivamente
> (FONTES, 2006, p. 20)

Conforme o autor supra, o investimento em segurança é necessário para que as informações sempre estejam disponíveis quando solicitadas, íntegras quando acessadas e em nível de confidencialidade para quem deva ter o acesso.

Políticas de Segurança da Informação

A Política de Segurança da Informação, também conhecida como PSI, é o documento que orienta e estabelece as diretrizes corporativas de uma determinada organização para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Para o Tribunal de Contas da União (TCU, 2012), a política de segurança da informação busca nortear a gestão de

ISSN: 2317-5265 – v. 9, n. 6 (2018) - UEMG - CLÁUDIO

segurança de informações. Ressalta-se que elas devem ser seguidas pela instituição para que sejam assegurados seus recursos computacionais e suas informações.

A política de segurança da informação está baseada nas recomendações propostas pela NBR ISO/IEC 27002 (ABNT, 2013), reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país. Diante deste cenário, a segurança da informação torna-se imprescindível para as organizações, sejam elas do setor público ou privado. Sem exceção de toda e qualquer organização, a segurança da informação deve estar interligada em cada atividade processada na empresa.

Para o TCU (2012), a Política de Segurança da Informação não deve ficar restrita à área de informática. Ela deve envolver os planos estratégicos do setor bem como as políticas institucionais. Ressalta-se que o conteúdo da Política de Segurança da Informação deve ser distinto de acordo com cada organização, seu perfil, nível de maturidade, grau de informatização, etc. Porém, lembra que alguns tópicos dela são comuns entre as organizações, tais como (2012, p.11):

- Definição de segurança de informações e de sua importância como mecanismo que possibilita o compartilhamento de informações;
- Declaração de comprometimento da alta administração com a PSI, apoiando suas metas e princípios;
- Objetivos de segurança da instituição;
- Definição de responsabilidades gerais na gestão de segurança de informações;
- Orientações sobre análise e gerência de riscos;
- Princípios de conformidade dos sistemas computacionais com a PSI;
- Padrões mínimos de qualidade que esses sistemas devem possuir;
- Políticas de controle de acesso a recursos e sistemas computacionais;
- Classificação das informações (de uso irrestrito, interno, confidencial e secretas);
- Procedimentos de prevenção e detecção de vírus

ISSN: 2317-5265 – v. 9, n. 6 (2018) - UEMG - CLÁUDIO

- Princípios legais que devem ser observados quanto à tecnologia da informação (direitos de propriedade intelectual, direitos de software, normas legais correlatas aos sistemas desenvolvidos, cláusulas contratuais);
- Princípios de supervisão constante das tentativas de violação de segurança de informações;
- Consequências de violações de normas estabelecidas na política de segurança;
- Princípios de gestão da continuidade do negócio;
- Plano de treinamento em segurança de informações (TCU, 2012, p.11).

Valor e importância

A política de segurança da informação está presente em diversos segmentos. Ela consiste como apoio de prevenção de fraudes e acessos indesejados nas plataformas do sistema das organizações. Esta política deve prever como deverá ser efetuado o acesso das informações de todas as formas possíveis, ou seja, internamente, externamente e quais tipos de mídia poderão transportar e ter acesso a esta informação, em evidencia nos casos, se destaca sistemas bancários, vítimas constantes por ataques nas plataformas de atendimento, fazendo com que os dados protegidos sejam corrompidos.

Para garantir a segurança e o controle, a empresa deve definir diretrizes, normas, ferramentas, procedimentos e responsabilidades aos profissionais que lidarão com essas informações. É o documento que determina as regras dentro da organização para uso de recursos tecnológicos e descarte de informações. Segundo Pinheiro (2009), a divulgação das informações confidenciais ou secretas pelos elementos que participam da organização constitui-se em uma falta ética e moral grave.

O elo mais frágil de um processo de segurança envolve as pessoas que utilizam as plataformas do sistema, que por sua vez, é a responsável por garantir a fidelidade da informação. Em um planejamento estratégico da informação é vital a participação do analista ou gestor, que é a pessoa quem tem competência para avaliar o valor da informação.

ISSN: 2317-5265 – v. 9, n. 6 (2018) - UEMG - CLÁUDIO

.

Práticas para segurança da informação

A melhor forma de garantir a segurança da informação é atuar junto às pessoas que, de alguma forma, manipulam a informação, conscientizando-as com treinamentos e utilizar termos de confidencialidade. Estes termos permitem responsabilizar juridicamente as pessoas que de alguma forma causar um dano financeiro à empresa por vazamento de informações sigilosas.

Não basta implantar políticas e métodos, é necessário o envolvimento das pessoas para o sucesso da implantação de uma Política de Segurança. Existem diversas formas de envolvê-los nesse processo. Segundo o TCU (2012), uma forma de envolver os colaboradores da organização sobre o valor da informação é através de normativos, manuais e procedimentos. Ainda, a promoção de encontros, seminários e palestras sobre o tema, bem como propagandas visuais de conscientização também ajuda no envolvimento. Vale ressaltar que ações de prevenção, cursos específicos, reciclagem e especializações são formas de alcançar e disseminar as Políticas de Segurança

Mais do que a proteção através dos dispositivos tecnológicos, o olhar atento ao fator humano é imprescindível. A maioria dos problemas nos sistemas relacionados à Segurança da Informação são causados pela utilização indevida e falta da política dos mesmos, pelas pessoas que interagem com os sistemas.

As empresas, juntamente com o setor de Recursos Humanos e Tecnologia da Informação, devem estar alinhadas no planejamento, elaboração e programação das reuniões para todos os usuários da informação com o objetivo central da segurança das informações.

Outras formas para minimização de riscos podem ser verificadas a seguir de acordo com Pinheiro (2009):

ISSN: 2317-5265 – v. 9, n. 6 (2018) - UEMG - CLÁUDIO

- Política da mesa limpa: deixando no ambiente de trabalho apenas o básico para a execução de tarefas, minimizando a perda de dados sigilosos ou confidenciais.
- Política da tela limpa: em caso de ausência no ambiente de trabalho, que o colaborador deixe bloqueada a estação de trabalho, minimizando riscos.
- Cuidados no compartilhamento de dados pessoais e/ou organizacionais, podendo expor vulnerabilidades ou informações importantes da organização.

Sendo assim, a Política de Segurança da Informação tem o objetivo de proteger as informações, conforme Albertin e Pinochet (2010) afirmam que as empresas estão dando maior ênfase aos aspectos relacionados à segurança, relacionamento com clientes e privacidade dos dados, sendo considerados até críticos para os negócios. Logo, toda e qualquer organização deve inteirar sobre essas ferramentas de suporte aos usuários a fim de mitigar riscos sobre suas informações.

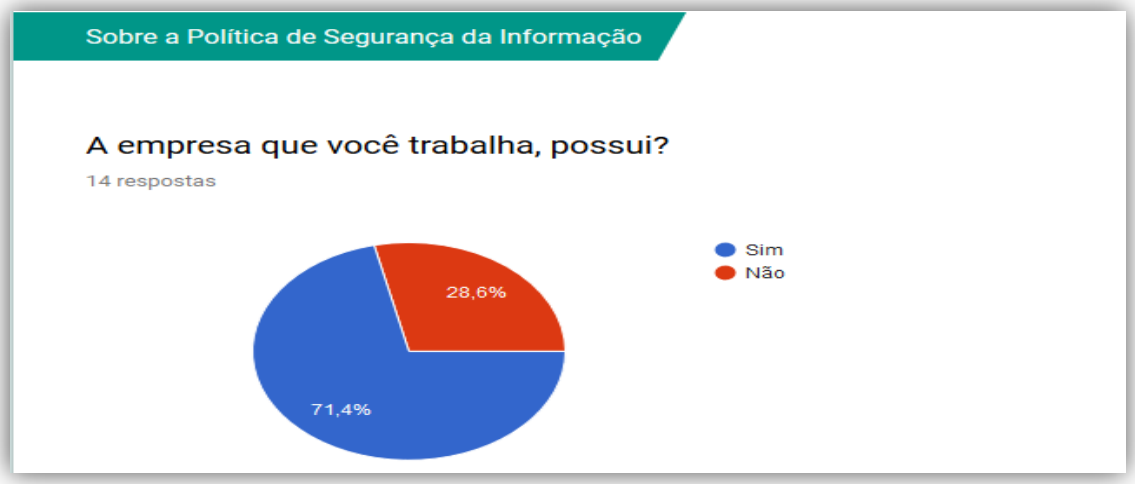
RESULTADOS E DISCUSSÃO

A primeira questão levantada aos funcionários foi sobre a existência de uma Política de Segurança da Informação própria da empresa. Conforme o gráfico apresentado a seguir, quatro colaboradores afirmaram que a empresa não possui a política e dez funcionários afirmaram que a empresa possui a política de segurança da informação.

Baseado nesse levantamento, os funcionários que julgaram que a empresa não possui Política de Segurança, não puderam mais responder às demais questões, pois o resultado seria impactado por uma amostra de respostas que sequer reconhece a presença de itens, podendo influenciar nos resultados dos que reconhecem a utilização da Política de Segurança da Informação (Gráfico 1).

ISSN: 2317-5265 – v. 9, n. 6 (2018) - UEMG - CLÁUDIO

Gráfico 1 – Política de Segurança da Informação na empresa pesquisada



Fonte: dados da pesquisa (2018)

Consideramos que apesar da grande maioria dos entrevistados afirmarem que sabem da existênciada Política de Segurança da Informação, um número considerável disse desconhecer sobre a mesma em ambiente de trabalho.

Para os funcionários que declinaram sobre a presença da Política de Segurança da Informação na organização, foi perguntado se os mesmos consideram importante o uso de políticas de conscientização sobre o valor da informação na empresa. As respostas são apresentadas no Gráfico 2 a seguir.

ISSN: 2317-5265 – v. 9, n. 6 (2018) - UEMG - CLÁUDIO

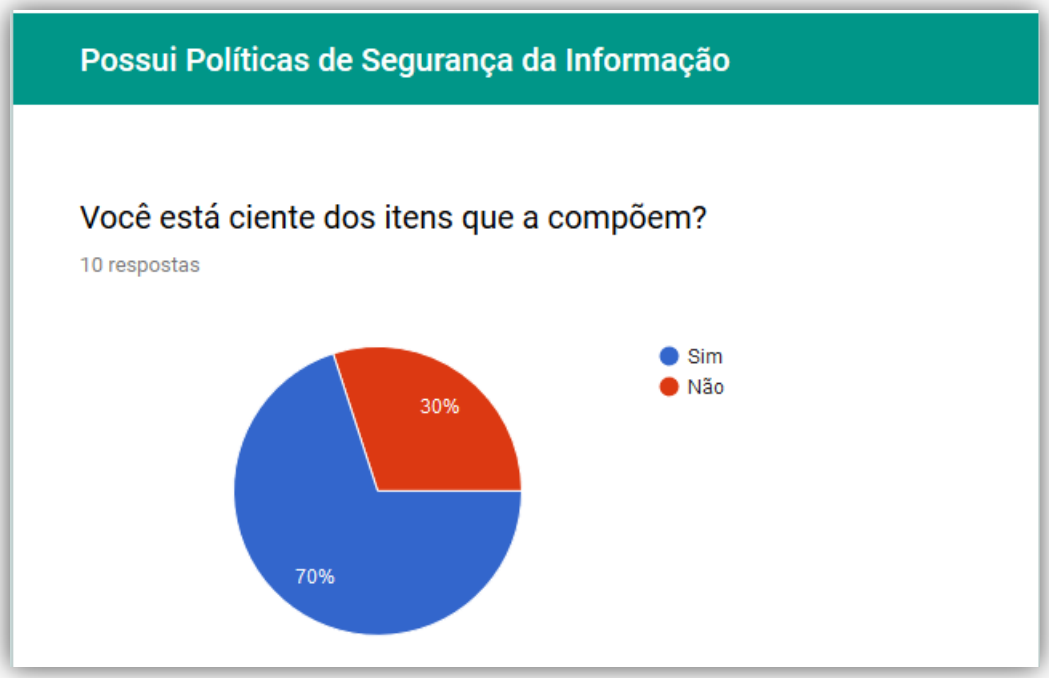
Gráfico 2 – Importância das Políticas de Segurança da Informação em uma organização

Fonte: dados da pesquisa (2018)

Conforme é possível analisar, todos os funcionários concordam sobre a importância do uso e utilização da Política de Segurança da Informação na empresa. Aos funcionários que afirmaram ter ciência que a empresa possui Política de Segurança da Informação, foram perguntados sobre a ciência dos itens que fazem parte da política. A seguir apresentamos os resultados (Gráfico 3).

ISSN: 2317-5265 – v. 9, n. 6 (2018) - UEMG - CLÁUDIO

Gráfico 3 – Ciência dos itens que compões as políticas de segurança da informação



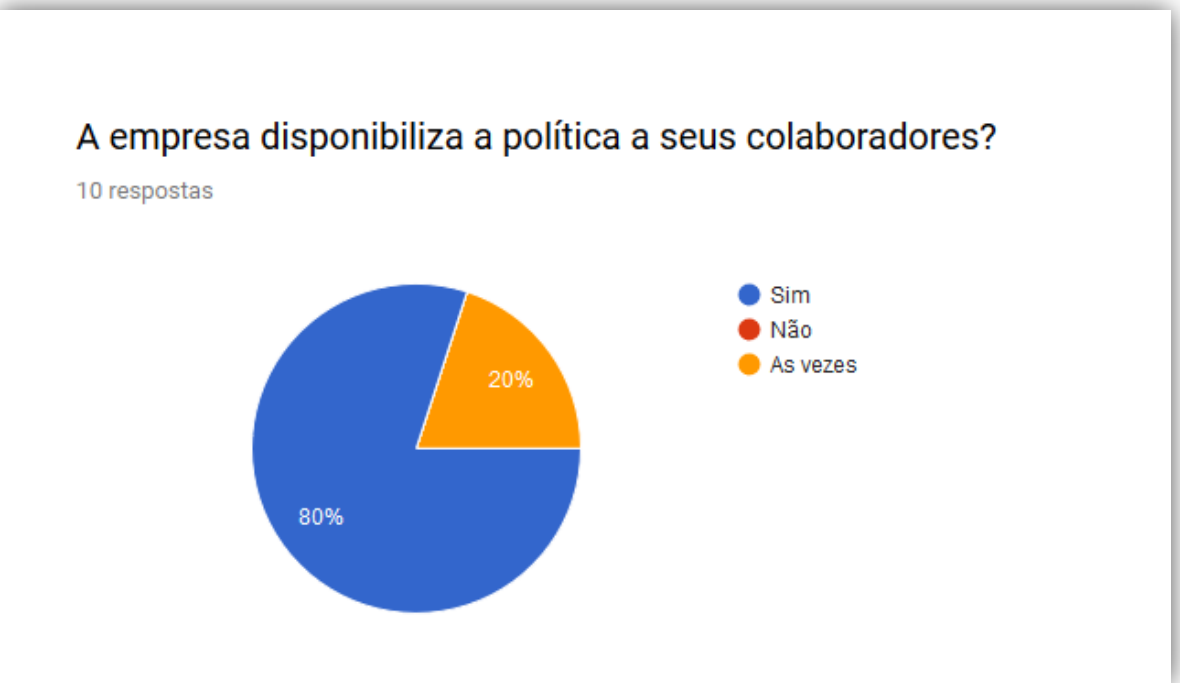
Fonte: dados da pesquisa (2018).

Conforme os dados acima, é possível afirmar que mesmo cientes que a empresa possui a política de segurança, nem sempre os funcionários possuem a ciência dos itens descritos nela, podendo gerar dúvidas e incertezas sobre a proteção, divulgação e guarda das informações da empresa.

Aos funcionários foi perguntado sobre a disponibilização daPolítica de Segurança da Informação. As respostas são consolidadas no Gráfico 4 adiante:

ISSN: 2317-5265 – v. 9, n. 6 (2018) - UEMG - CLÁUDIO

Gráfico 4 – Disponibilização das políticas de segurança da informação



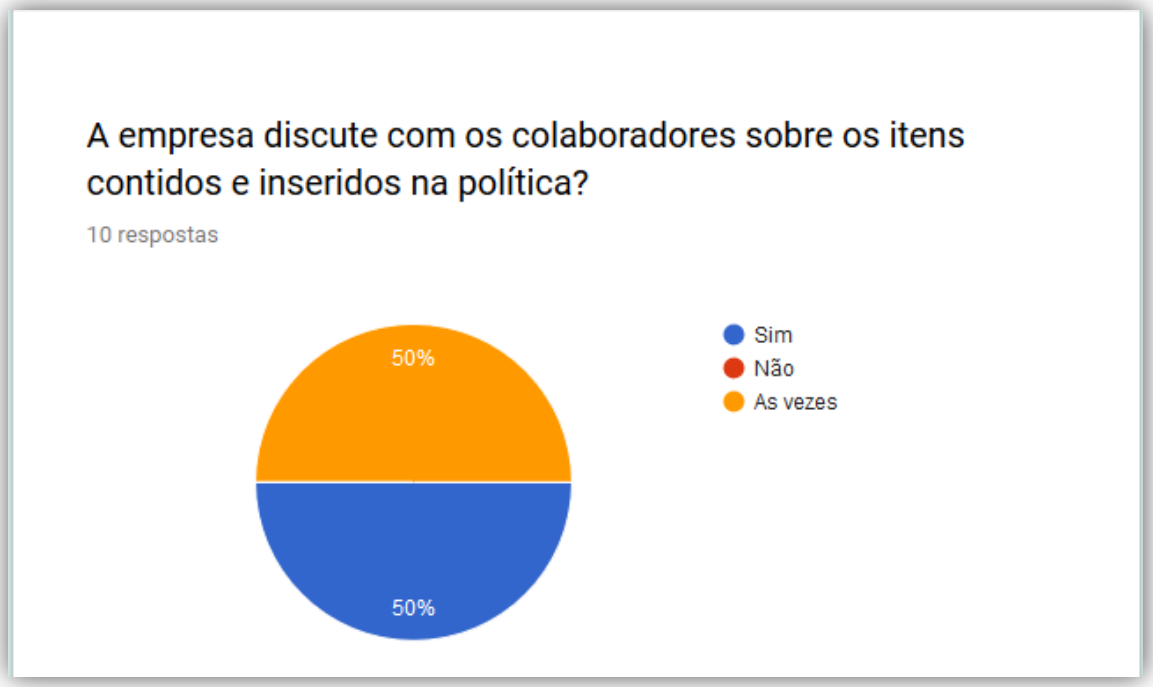
Fonte: dados da pesquisa (2018)

Conforme os resultados, é possível afirmar que alguns funcionários ainda se mostram incertos da disponibilização da Política de Segurança da Informação. Percebe-se então que poderiam ser feitas algumas ações que divulgassem mais a política e como o funcionário pode encontrá-la, seja em mídia digital, manual ou em outras formas.

Aos funcionários foi questionado ainda sobre os itens contidos na Política de Segurança da Informação da empresa, sendo as respostas obtidas e discriminadas no Gráfico 5, a seguir.

ISSN: 2317-5265 – v. 9, n. 6 (2018) - UEMG - CLÁUDIO

Gráfico 5 – Discussão sobre os itens contidos nas políticas de segurança da informação



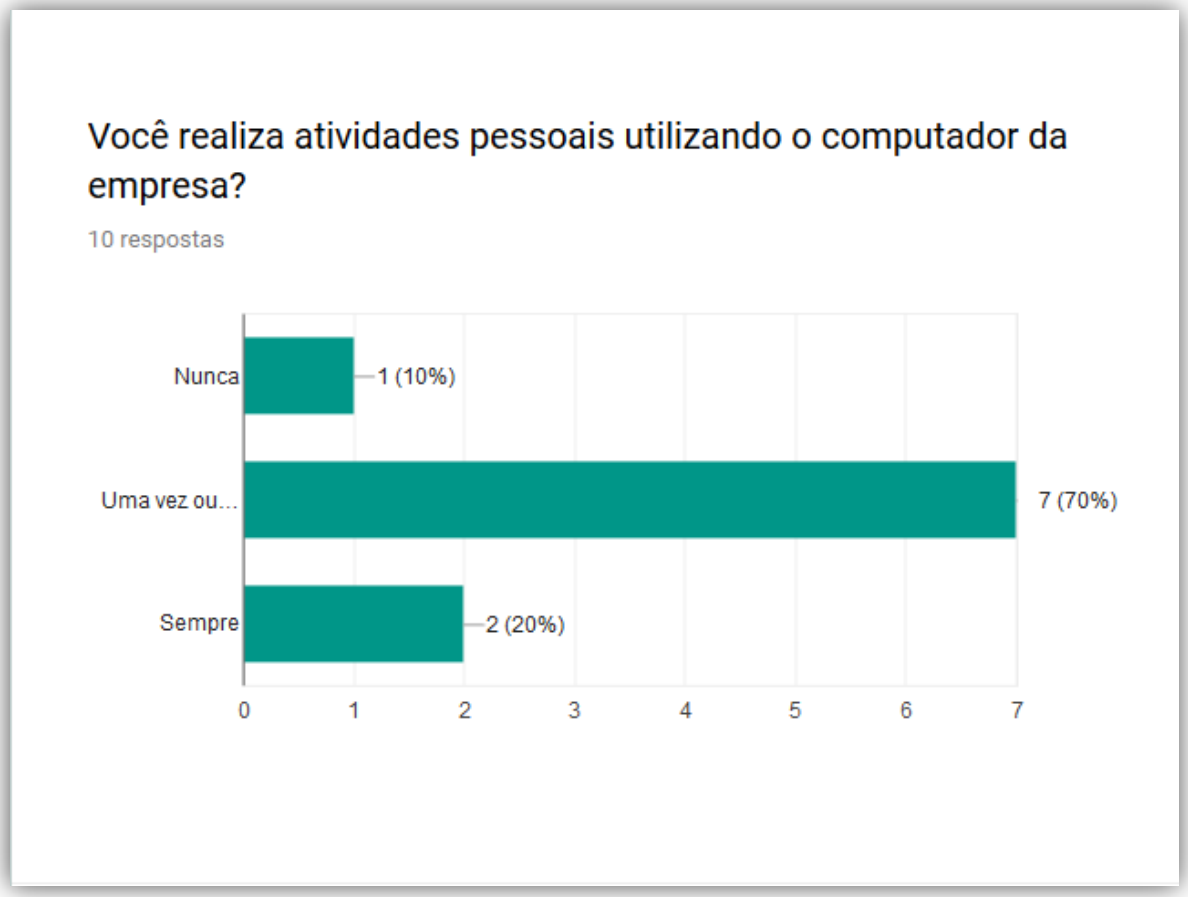
Fonte: dados da pesquisa (2018)

Conforme as respostas do gráfico 5, percebeu-se que nem sempre os funcionários discutem sobre os itens contidos na Política de Segurança da Informação da empresa. Ações de educação interna devem ser executadas neste sentido.

Continuando, aos funcionários foi questionado sobre o uso de atividades pessoais utilizando os computadores da empresa. As respostas são apresentadas a seguir, como descritas no Gráfico 6.

ISSN: 2317-5265 – v. 9, n. 6 (2018) - UEMG - CLÁUDIO

Gráfico 6 – Utilização dos computadores da empresa para atividades pessoais



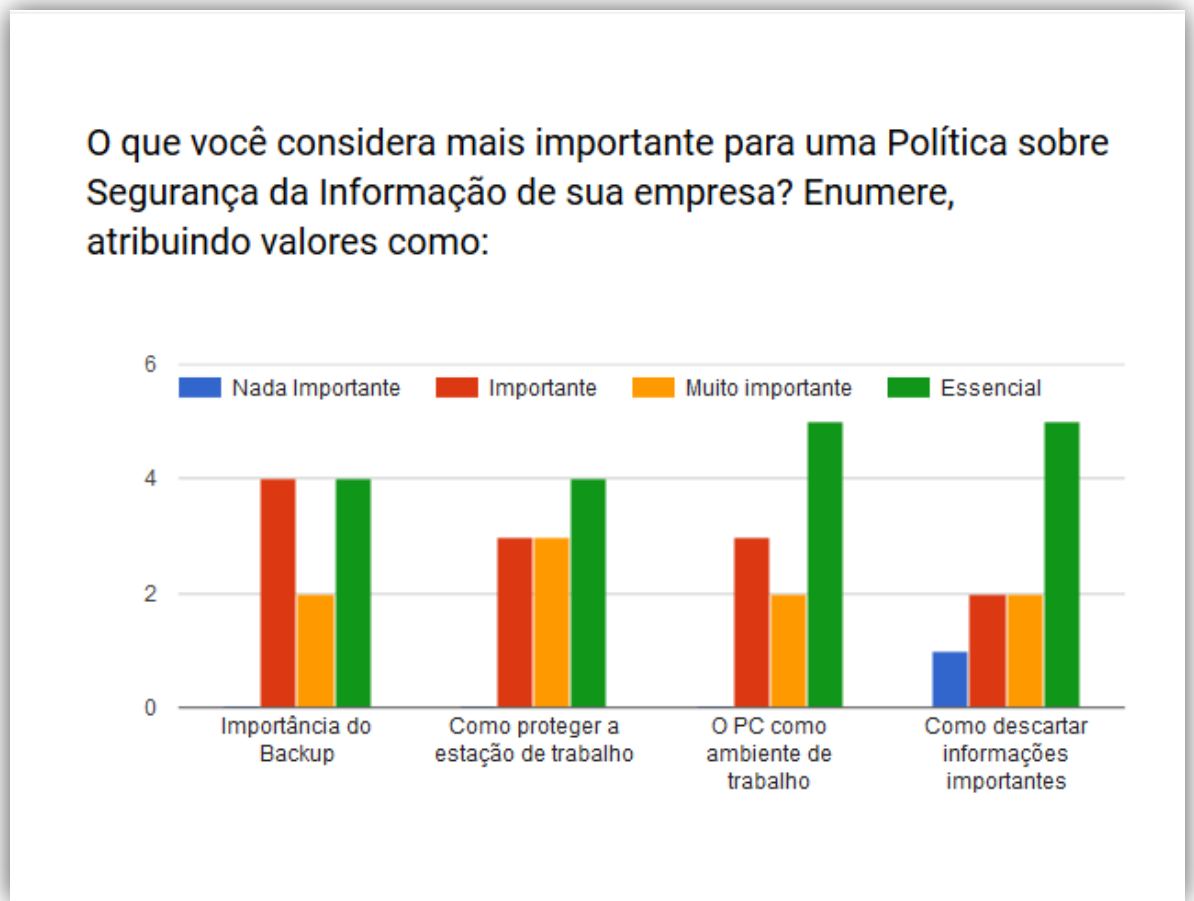
Fonte: dados da pesquisa dos autores

Conforme as respostas obtidas no gráfico 6, podemos afirmar que a utilização da estação de trabalho com fins pessoais ainda é uma atividade muito comum pelos funcionários. Os números encontrados nesse gráfico alertam sobre os riscos que uma empresa corre quando seus funcionários trafegam dados pessoais em sistemas empresariais, que podem estar sem a proteção devida, corrompendo os sistemas operacionais.

Aos funcionários foi perguntado sobre itens que considerem importantes em uma Política de Segurança da Informação. A seguir foram apresentados os resultados, como discriminados no Gráfico 7.

ISSN: 2317-5265 – v. 9, n. 6 (2018) - UEMG - CLÁUDIO

Gráfico 7 – Itens importantes de uma política de segurança da informação



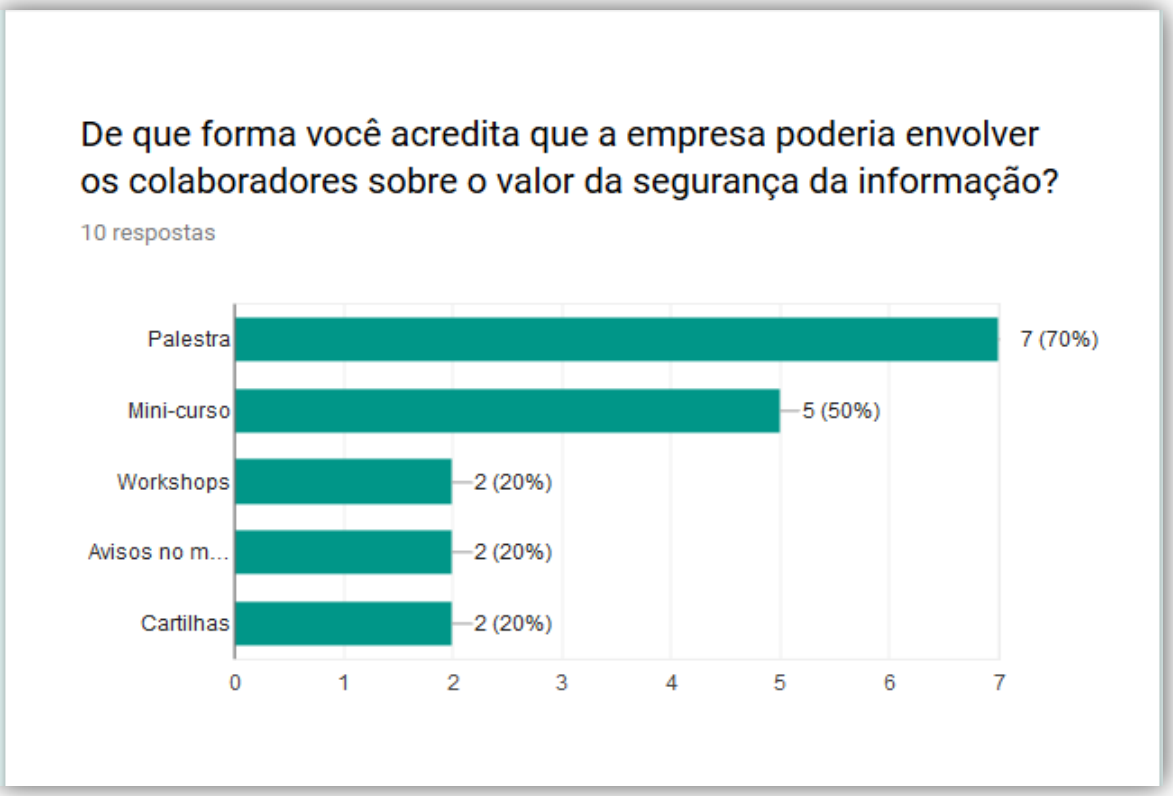
Fonte: dados da pesquisa (2018)

Conforme o gráfico, podemos afirmar sobre os itens considerados mais importantes em uma Política de Segurança, a presença maior do item “essencial”, apesar do conflito de respostas descritos no Gráfico 6, acima. Também, verifica-se que ainda não está consolidada um pensamento de segurança em razão das respostas da importância do *backup*, da proteção da estação de trabalho e do descarte de informações, face a essencialidade de segurança nas informações e a gradação de importância dada pelos funcionários

ISSN: 2317-5265 – v. 9, n. 6 (2018) - UEMG - CLÁUDIO

Aos funcionários foi perguntado sobre formas de envolver os colaboradores sobre o valor da segurança da informação para a empresa. A seguir apresentamos os resultados.

Gráfico 8 – Envolvimento dos funcionários sobre o valor da segurança da informação na empresa.



Fonte: dados da pesquisa dos autores

Conforme as respostas, podemos afirmar que a maior parte dos colaboradores deseja receber informações através de palestras ou minicursos com o objetivo de se capacitarem, o que se mostra um excelente indicador de ações.

Aos funcionários foi perguntado sobre ações de conscientização que a empresa pode desenvolver aos clientes. Como se trata de uma questão discursiva, a seguir apresentamos as respostas que julgamos mais relevantes.

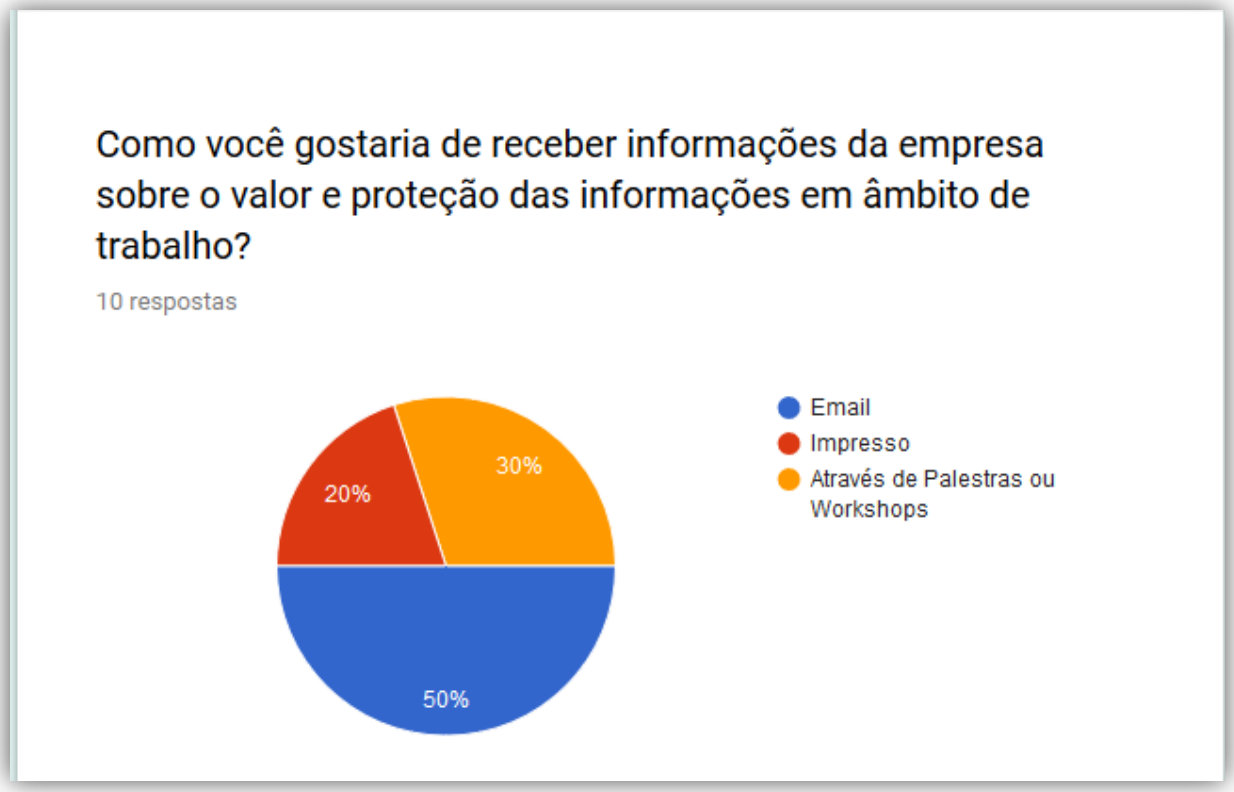
ISSN: 2317-5265 – v. 9, n. 6 (2018) - UEMG - CLÁUDIO

> *"Através de Informativos via e-mail, mensagens SMS, destacando a importância da segurança digital, já que é um meio que cresce significativamente." Funcionário 01*
> *"Sim, e necessário a conscientização para que todos possam ter conhecimentos adequados e dessa forma manter o sigilo e segurança das informações." Funcionário 02*
> *"Através de material impresso" Funcionário 03 (*dados da pesquisa, 2018)

Pode-se afirmar que a divulgação da importância da proteção das informações é o item mais presente nas respostas dos funcionários.

Aos funcionários foi perguntado de qual forma eles gostariam de receber informações sobre formas e maneiras de proteger as informações. As respostas são apresentadas no gráfico a seguir.

Gráfico 9 – Formas de divulgar as informações da empresa sobre segurança da informação.



ISSN: 2317-5265 – v. 9, n. 6 (2018) - UEMG - CLÁUDIO

Fonte: dados da pesquisa (2018).

Sobre os números apresentados no gráfico, podemos afirmar que os funcionários estão divididos entre os que preferem receber remotamente as informações, via endereço eletrônico e os que preferem materiais físicos, palestras e workshops.

CONCLUSÃO

Concluímos através dos resultados apresentados que mesmo para as empresas que já utilizam Políticas de Segurança da Informação, esse ainda é um assunto que merece maior atenção e deve ser divulgado entre os funcionários das empresas. Percebemos muitas dúvidas entre os funcionários sobre a existência da política e sobre o material apresentado no manual da empresa.

Podemos também perceber pela pesquisa que é um assunto que a maioria dos funcionários considera ser importante para ser debatido dentro da empresa e que são necessárias ações como palestras, minicursos e materiais impressos, exemplificadamente, para a divulgação de medidas de segurança dentro da empresa, sendo essas ações consideradas formas eficazes de proteção e de divulgação realizado no ambiente de trabalho pelos funcionários.

Verificamos também que o uso dos computadores das estações de trabalho da empresa é feito de forma irregular para atividades particulares, sendo comum essa prática no local e que merece uma maior atenção quanto ao uso.

Acreditamos que esse é um tema que merece importância dentro das empresas devido ao número crescente de informações que são produzidas por meios eletrônicos e que a proteção das informações é essencial tanto para a empresa quanto para os clientes.

REFERÊNCIAS

ALBERTIN, A. L.; PINOCHET, L. H. C. **Política de Segurança de Informação.** 1. ed. Rio de Janeiro: Elsevier, 2010. v. 1. 328 p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR 6023: Informação e documentação: Referências**. Rio de Janeiro, p. 24. 2002.

_____, **NBR ISO/IEC 27002: Tecnologia da informação. Técnicas de segurança. Código de prática para a gestão da segurança da informação.** Rio de Janeiro, p. 112. 2013.

BRASIL. Tribunal de Contas da União. **Boas Práticas em Segurança da Informação** / Tribunal de Contas da União. – 4. ed. – Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012.

CAMPOS, A. **Sistemas de Segurança da Informação**. 2 ed. Florianópolis: Visual Books, 2007.

FONTES, E. **Segurança da Informação:** o usuário faz a diferença**.** 1ªedição. São Paulo: Saraiva, 2006.

FONSECA, P. F. **Gestão de Segurança da Informação:** O Fator Humano. Curitiba, 2009. Disponível em:<www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/Paula Fernanda Fonseca - Artigo.pdf> Acesso em: 18 ago. 2018.

MARCONI, M. de A.; LAKATOS, E. M. **Fundamentos de Metodologia Cientifica**. 7. ed. São Paulo: Atlas, 2010, 249 p.

PINHEIRO, J. M. S. Auditoria e Análise de Segurança da Informação - **Segurança Física e Lógica. (2009). Disponível em: <www.projetoderedes.com.br/aulas/ugb_auditoria_e_analise/ugb_apoio_auditoria_e_analise_de_seguranca_aula_02.pdf.pdf> Acesso em: 18 ago. 2018.**

PRODANOV, C. C.; FREITAS, E. C. de. Metodologia do Trabalho Científico: **Métodos e Técnicas da Pesquisa do Trabalho Acadêmico. 2. Ed. Novo Hamburgo: Universidade Feevale, 2013.**

SÊMOLA, M. **Gestão da Segurança da Informação**. 1. Ed. Rio de Janeiro: Campus, 2003.