O IMPACTO DE AÇÕES DE CONSCIENTIZAÇÃO NA SEGURANÇA DA INFORMAÇÃO

ARTIGO ORIGINAL

TRIGOS, Maria Luciana¹, NUNO, Claudinei Di²

TRIGOS, Maria Luciana. NUNO, Claudinei Di. **O impacto de ações de conscientização na segurança da informação.** Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano. 06, Ed. 10, Vol. 03, pp. 46-72. Outubro 2021. ISSN: 2448-0959, Link de acesso: <https://www.nucleodoconhecimento.com.br/administracao/acoes-de-conscientizacao>, DOI: 10.32749/nucleodoconhecimento.com.br/administracao/acoes-de-conscientizacao

RESUMO

Com o avanço da tecnologia e a eclosão da internet, a troca de recursos e informações é cada vez mais frequente no âmbito organizacional. Embora o compartilhamento de recursos facilite a operacionalidade da empresa, não há dúvidas que também favorece a exposição a riscos de segurança da informação. Para atingir níveis confiáveis de segurança, as empresas preocupam-se prioritariamente com as tecnologias e os processos, subestimando os recursos humanos. Por outra parte, nota-se que a maioria das violações de segurança da informação são causadas por falhas humanas associadas à desinformação. Nesse contexto, ações de conscientização em segurança da informação são importantes na medida em que podem reduzir os riscos de incidentes que têm origem nas condutas das pessoas. Assim, o artigo pretende responder a seguinte pergunta: até que ponto as ações de conscientização em segurança da informação podem mudar o comportamento das pessoas no sentido de torná-lo mais aderente às boas

¹ Especialista em Gestão Estratégica da Tecnologia da Informação. Especialista em Direito Público com ênfase em Gestão Pública. Bacharel em Administração. Bacharel em Gastronomia.

² Orientador.

práticas de segurança da informação? Nesse sentido, o estudo visa descrever os resultados das ações de conscientização em segurança da informação implementadas no Serviço Federal de Processamento de Dados (Serpro), empresa pública de Tecnologia da Informação. Por meio de questionário foi verificado o engajamento dos empregados quanto às melhores práticas em segurança da informação propiciadas pelas referidas ações de conscientização, confrontando-o com as diretrizes da política de segurança da informação da empresa. Os resultados mostraram que a maioria dos respondentes está aderente às boas práticas de segurança da informação. Todavia, existem lacunas que confirmam a necessidade de futuras ações de conscientização. A partir da análise dos resultados concluiu-se que as ações de conscientização são fundamentais tanto para internalizar a política de segurança da informação de uma empresa como para promover o comportamento seguro dos colaboradores.

Palavras-chave: Segurança da Informação, Ações de Conscientização, Melhores Práticas.

1. INTRODUÇÃO

Cada vez mais, o compartilhamento de recursos e informações torna-se algo inevitável para a maioria das organizações. A evolução da tecnologia e a globalização foram fatores que propiciaram essa tendência. Os benefícios que essa conectividade proporciona para as organizações são inumeráveis, mas, por outro lado, a exposição aos riscos à segurança da informação aumenta consideravelmente.

É possível afirmar que os dados e as informações de uma instituição integram seu patrimônio intangível, configurando-se verdadeiros ativos, imprescindíveis para a tomada de decisões estratégicas. Por tanto, a segurança da informação torna-se um ponto crucial para a sobrevivência das instituições, pois esta área de conhecimento é incumbida de proteger, tanto de forma física como lógica, o principal ativo da organização, a informação.

RC: 98717

Disponível em: <https://www.nucleodoconhecimento.com.br/administracao/acoes-de-conscientizacao>

O que se verifica na literatura é que as empresas, no intuito de minimizar as falhas na segurança da informação, dedicam seus maiores esforços às questões técnico-operacionais, prestando menor atenção ao papel dos recursos humanos. A crença de que a Segurança da Informação pode ser obtida com tecnologia correta e processos bem implementados foi sistematicamente derrubada a partir de situações em que os incidentes foram causados por pessoas que desligaram controles, ignoraram avisos ou deixaram de executar procedimentos e protocolos previamente estabelecidos. Assim, para garantir a salvaguarda das informações organizacionais, é de vital importância entender o comportamento humano individual e coletivo, suas atitudes sobre segurança da informação e a relação desses fatores com a cultura organizacional.

É evidente então que, ao instaurar uma Política de Segurança da Informação (PSI), a empresa deve contemplar, entre outros ativos suscetíveis ao risco, os recursos humanos, que são comprovadamente o elo mais frágil de toda a cadeia de proteção. O comportamento que as pessoas apresentem em relação à segurança das informações é fundamental, tendo em conta que o sucesso dos programas dependerá em grande medida do comprometimento que elas tenham quanto ao cumprimento das boas práticas em segurança. Nesse sentido investir em conscientização em segurança da informação pode trazer grandes benefícios para a empresa.

Observa-se que a literatura não é prolífica quando se trata de estudos que abordem a análise e mensuração dos resultados de programas de conscientização em segurança da informação e por isso, o estudo visa contribuir proporcionando instrumentos de pesquisa para sanar uma lacuna teórico-científica identificada com base em um mapeamento bibliográfico que apontou a escassez de trabalhos acerca do tema.

Assim, o artigo pretende responder a seguinte pergunta: até que ponto as ações de conscientização em segurança da informação podem mudar o comportamento das

pessoas no sentido de torná-lo mais aderente às boas práticas de segurança da informação?

Nesse sentido, o estudo visa descrever os resultados das ações de conscientização em segurança da informação, implementadas em uma empresa pública de Tecnologia da Informação, o Serviço Federal de Processamento de Dados (Serpro), Regional Florianópolis. Para isso, são consideradas as ações realizadas no período compreendido entre julho de 2016 a abril de 2020.

Por meio de questionário será verificado o engajamento dos empregados quanto às melhores práticas em segurança da informação propiciadas pelas referidas ações de conscientização, confrontando-o com as diretrizes da política de segurança da informação do Serpro. A partir do questionário também será possível identificar as preferências dos colaboradores quanto aos meios utilizados para a promoção da conscientização em segurança da informação, objetivando a obtenção de referências para o planejamento de futuras ações.

2. FUNDAMENTAÇÃO TEÓRICA

2.1 SEGURANÇA DA INFORMAÇÃO

A evolução tecnológica contribui para que as organizações automatizem seus serviços, em prol de uma maior eficiência e eficácia. Em contrapartida, o aumento da conectividade demanda cuidados frente às ameaças às quais se expõem os sistemas de informação e comunicação, especialmente quando conectados à rede mundial de computadores (UNIVERSIDADE DE BRASÍLIA, 2010, p. 27).

Assim, a Segurança da Informação, como área de estudo, passa a ocupar um lugar de destaque. A sua importância não está mais limitada apenas ao aprimoramento de ferramentas para a detecção de invasão e proteção das informações, senão ao estudo de medidas voltadas para a prevenção, detecção, resposta, recuperação e continuidade do negócio (DANTAS, 2011, p. 6).

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT) define os três principais critérios que norteiam a segurança da informação, conhecidos como CID: Confidencialidade, Integridade e Disponibilidade. A confidencialidade é a capacidade que um sistema tem de permitir que apenas a pessoa autorizada possa ter acesso a determinadas informações; a integridade garante que uma informação seja verdadeira, ou seja, que não tenha sido corrompida ou alterada de maneira ilegal e a disponibilidade é o requisito que uma vez cumprido permite que as informações estejam disponíveis na hora certa para as pessoas certas (CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL, 2018, on-line).

Todos os mecanismos orientados a satisfazer esses princípios básicos precisam ser implementados na Política de Segurança da Informação (PSI) da empresa, que norteará a gestão de segurança das informações por meio de normativos que devem ser observados pelo corpo técnico e gerencial e pelos usuários internos e externos (BRASIL, 2012, p. 8). A Política de Segurança da Informação refere-se à “política que governa a abordagem da organização quanto ao gerenciamento de segurança da informação” (AXELOS, 2011, p. 61).

A definição de regras por escrito é fundamental para a constituição da PSI, no entanto, não garantem por si só, o cumprimento das boas práticas. Por isso, é necessário orientar os colaboradores a cumprir essas regras garantindo que todos entendam o motivo de cada normativa e se sintam comprometidos com a segurança da informação (FONSECA, 2009, p. 7).

A ausência de uma cultura da segurança das informações cria um ambiente propício para ataques e invasões que se servem das vulnerabilidades da empresa. A fuga das informações e a sua exposição involuntária ocorrem em momentos simples do dia a dia da empresa, o que torna os recursos humanos uma das maiores preocupações para a implementação de políticas e treinamentos voltados para a proteção das informações (DANTAS, 2011, p. 25).

Por isso a importância da participação da alta administração nas atividades relacionadas a segurança da informação e na formação de uma cultura organizacional baseada em regras bem definidas e conhecidas para garantir que os funcionários adquiram comportamentos que reduzam os riscos de atitudes negligentes ou maliciosas (ARAÚJO, 2018, p. 52).

Nesse sentido, a orientação e a informação são essenciais para a redução de riscos, devendo-se atentar para a importância do fluxo mostrado na Figura 2:

Figura 1 - Sequência para a mudança de conduta e prevenção dos riscos

Fonte: Coelho (2013, p. 89).

Um ponto importante a destacar é que conscientização não é treinamento. O propósito da conscientização é simplesmente focar a atenção em segurança. A conscientização tem a intenção de alertar os indivíduos para reconhecer situações de segurança de TI e agir corretamente (WILSON; HASH, 2003, p. 8).

Para Dourado; Alves (2016, p. 12) as ações devem fazer com que as pessoas compreendam e respeitem as políticas e princípios de segurança da informação, sejam conscientizadas da sua responsabilidade pela proteção das informações e encorajadas a praticar a segurança em suas operações diárias.

2.2 SEGURANÇA DA INFORMAÇÃO EM RECURSOS HUMANOS

Uma Política de Segurança de Informação (PSI) eficiente deve ser instaurada com base nas recomendações propostas pela norma ABNT NBR ISO/IEC 27001, reconhecida em todas as partes do mundo como referência para a gestão da segurança da informação. Esta norma define os requisitos para estabelecer,

implementar, manter e melhorar continuamente um Sistema de Gerenciamento de Segurança da Informação (PORTAL GSTI, 2020, on-line).

Especificamente, no que tange à segurança dos recursos humanos, a ISO/IEC 27001 aponta como responsabilidades da organização, o treinamento, a conscientização e a competência das pessoas responsáveis, indicando que “A organização deve também assegurar que todo o pessoal pertinente esteja consciente da relevância e importância das suas atividades de segurança da informação e como eles contribuem para o alcance dos objetivos do SGSI” Associação Brasileira de Normas Técnicas (2013a, p. 10).

Em sintonia com a ISO 27001, a ISO 27002 vem fortalecer a importância da conscientização, educação e treinamento em segurança da informação, estabelecendo que “Convém que todos os funcionários da organização e, onde pertinente, partes externas recebam treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções” Associação Brasileira de Normas Técnicas (2013b, p. 13).

É importante ressaltar que as ações de conscientização precisam ser contínuas e atualizadas periodicamente, de modo que permaneçam alinhadas com as políticas e os procedimentos da organização, e sejam construídas com base nas lições aprendidas dos incidentes de segurança da informação (FONSECA, 2009, p. 8).

Quanto aos tipos de treinamento em conscientização, a norma recomenda atividades diversificadas, como campanhas, publicação de boletins, folhetos, palestras, entre outras. Sugere-se também a utilização de diferentes formas de apresentação, incluindo treinamento presencial, treinamento à distância, treinamento baseado em web, autodidata, entre outros (FONTES, 2015, p. 105).

A norma destaca que ao compor um programa de conscientização, é importante não focar apenas no “o que” e “como”, mas também no “por que”, pois é importante que os funcionários entendam o impacto potencial, positivo e negativo, do seu próprio

comportamento na organização e que a participação deles beneficiará não apenas a empresa, mas também as suas próprias informações. (FONSECA, 2009, p. 7).

Para Cunha, dificilmente se consegue o comprometimento de alguém que não sabe ou não entende o que se requer dele num ambiente corporativo, e quais são os perigos e ameaças a que ele está sujeito. Todo processo ‘mensurável’ de aprendizado deveria necessariamente começar com a conscientização (CUNHA, 2007, p. 43).

Por último, ressalta-se a importância de realizar uma avaliação dos programas ou ações de conscientização para obter uma base para o planejamento de futuras ações que tenham como foco a melhoria contínua (FONTES, 2015, p. 106).

2.3 GOVERNANÇA DE TI E AS MELHORES PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO

A informação é um ativo essencial das organizações para a tomada de decisões estratégicas e por isso os aspectos relacionados à segurança da informação são críticos para o sucesso dos negócios e a competitividade corporativa. Nesse sentido, a governança de Tecnologia da Informação (TI) cumpre um rol fundamental.

Para o IT Governance Institute (2007, p. 7)

A governança de TI integra e institucionaliza boas práticas para garantir que a área de TI da organização suporte os objetivos de negócios. Além disso, habilita a organização a obter vantagens de sua informação, de forma a maximizar os benefícios, capitalizar as oportunidades e viabilizar o ganho de poder competitivo.

Assim, a governança de TI reúne especificações que servem de apoio para a tomada de decisões, estimulando comportamentos e ações adequados em relação ao uso dos recursos de TI (IT GOVERNANCE INSTITUTE, 2007, p. 7). Ou seja, em sua essência, a governança de TI, é um conjunto de regras e melhores práticas que, adaptadas à cultura organizacional, servirá para profissionalizar a gestão da TI,

visando transformá-la em instrumento de apoio às decisões de negócio (WUNSCH, 2010, p. 8).

O aumento da maturidade empresarial tem levado as organizações a buscar a implantação de métodos e práticas bem-sucedidas, tais como os *frameworks* COBIT (*Control Objectives for Information Technologies*) e o ITIL (*Information Technology Infrastructure Library*) (WUNSCH, 2010, p.9-10), que somados às normas ISO 27001 e 27002 formam uma base robusta para a governança e a gestão dos serviços de TI.

No COBIT 5, o habilitador Princípios, políticas e frameworks descreve os veículos utilizados pela gestão para traduzir o comportamento desejado dos colaboradores para com a segurança da informação, apresentando orientações formais, porém práticas, relacionadas às atividades desenvolvidas no dia a dia. Já, no ITIL, as boas práticas da segurança da informação aparecem na segunda fase de implementação da ITIL, o desenho dos serviços (*Service Design*), que foca na confidencialidade, integridade e disponibilidade da informação no contexto dos negócios e processos de negócio. (RIOS; RIOS; TEIXEIRA FILHO, 2017, p. 137-138).

3. DESENVOLVIMENTO

A pesquisa foi desenvolvida na Regional Florianópolis do Serviço Federal de Processamento de Dados (Serpro), empresa pública brasileira de prestação de serviços em tecnologia da informação. O estudo objetiva descrever os resultados das ações de conscientização em segurança da informação que compõem o Programa Regional Segura, realizadas pelo Grupo de Trabalho Segurança da Informação – Regional Florianópolis (GT). A pesquisadora pertence ao quadro de empregados do Serpro, atua na área operacional (SUPOP) e faz parte do GT desde 2017.

A partir do levantamento das ações realizadas, foram elaborados os itens do questionário, visando constatar o engajamento dos empregados quanto às melhores

práticas em segurança da informação propiciadas pelas referidas ações. As respostas do questionário foram analisadas triangularmente considerando as normativas da política de segurança da informação do Serpro e a teoria que embasa o estudo.

3.1 LEVANTAMENTO DAS AÇÕES REALIZADAS

O Programa Regional Segura foi criado a meados de 2016 na Regional Florianópolis do Serpro com os seguintes objetivos: estar aderente às diretrizes de segurança da informação do SERPRO, ser uma regional de referência em segurança da informação e gerar valor, por meio de suas ações, aos serviços prestados pela regional, melhorando os indicadores atuais.

Com esse intuito criaram-se o Grupo de Trabalho Segurança da Informação – Regional Florianópolis (GT), integrado por empregados de distintas áreas da regional e a Comissão Regional de Segurança – Florianópolis, formada pelos gerentes dessas áreas.

O GT orienta seus esforços para a realização de ações de natureza técnico-operacional, com foco nos recursos tecnológicos e nos processos, e de conscientização, com ênfase nos recursos humanos. As ações de conscientização, assunto deste artigo, foram realizadas pelo GT de diversas formas dentro do período compreendido entre julho de 2016 e abril de 2020, conforme mostra o Quadro 1.

Quadro 1 - Ações de Conscientização

Ações realizadas em 2016
Divulgação de dicas com bombons.
Palestra de especialista sobre a política de segurança do Serpro.
Palestra de especialista sobre técnicas de engenharia social.
Ações realizadas em 2017
Divulgação de vídeo sobre senhas seguras.

Dicas em formato de tirinhas sobre descarte seguro de documentos, publicadas no boletim Primeira Leitura.*
Workshop sobre a norma SG005 do Serpro e a Lei de Acesso à Informação (LAI).
Dicas em formato de texto sobre categorização das informações publicadas no boletim Primeira Leitura.
Curso de Gestão da Segurança da Informação.
Quiz sobre fragmentação de documentos sigilosos, veiculado no boletim Primeira Leitura.
Cinema na Regional Segura.
1º Serpro Security Week.**
Cartazes com dicas de conexão segura de WI-FI colocados em locais estratégicos.
Ações realizadas em 2018
Artigo “Evidências nas nuvens”, publicado na revista Tema.
Artigo “Proteção do conhecimento em desenvolvimento de software”, publicado na revista Tema.
Matéria “Dicas de segurança: como combater o Spam?”, publicada no boletim Primeira Leitura, em nível nacional.
Mural da copa com dicas sobre segurança da informação.
Dicas e vídeo sobre a prática “Mesa limpa e tela limpa”, publicados no boletim Primeira Leitura.
2º Serpro Security Week, com participação de outras regionais e transmissão nacional.
Ações realizadas em 2019
Capacitação em segurança da informação para a integração de jovens aprendizes.
Prática “Mesa limpa e Tela limpa”. Análise da situação real das estações de trabalho em relação às boas práticas de segurança da informação.
3º Serpro Security Week, com participação de outras regionais e transmissão

nacional. Inclusão de sala de escape na programação.
Cartaz sobre a troca de PIN para imprimir documentos sigilosos.
Cartilhas do CERT.BR nos eventos distribuídas nos eventos.
Ações realizadas em 2020
Dicas de segurança em formato digital por meio do Serprocards.
* Boletim Primeira Leitura é o informativo corporativo de publicação diária.
** O Serpro Security Week é um evento criado e produzido pelo GT que dedica uma semana inteira do ano para abordar conteúdos exclusivos de segurança da informação, por meio de palestras, workshops, sala de escape, etc.

Fonte: autoria própria.

3.2 ELABORAÇÃO E APLICAÇÃO DO QUESTIONÁRIO

O questionário foi composto de trinta e dois itens. Em trinta deles o respondente devia escolher a opção que melhor representasse a sua opinião, utilizando a seguinte escala de concordância: concordo totalmente, concordo parcialmente, não concordo nem discordo, discordo parcialmente, discordo totalmente. Nos dois restantes, o respondente podia marcar todas as opções que considerasse necessárias.

Cada ação de conscientização realizada gerou, pelo menos, um item. Os itens, por sua vez, foram agrupados em 10 seções, de acordo à similaridade do assunto, a saber: sobre as ações de conscientização realizadas no período de 2016 a 2020, sobre engenharia social, sobre senha segura, sobre categorização da informação, sobre conexão segura, sobre segurança na estação de trabalho, sobre segurança no recebimento de e-mails, sobre segurança na impressão de documentos, sobre meus conhecimentos em segurança da informação e sobre os meios de conscientização para ações futuras. O respondente ainda devia informar a sua lotação, a sua faixa etária, se tinha ou não função gerencial e o seu cargo. O questionário deixava explícita a garantia de anonimato e sigilo das respostas.

RC: 98717

Disponível em: <https://www.nucleodoconhecimento.com.br/administracao/acoes-de-conscientizacao>

3.3 ANÁLISE DOS RESULTADOS

O questionário foi aplicado entre os dias 5 a 14 de agosto de 2020. Foram convidados a participar 110 colaboradores e responderam 32, o que indica que a percentagem de colaboradores convocados que atenderam à pesquisa foi em torno de 29%. No Anexo I apresenta-se cada item do questionário junto ao respectivo gráfico gerado pelas respostas dos participantes.

A seção “Sobre as ações de conscientização realizadas no período de 2016 a 2020” foi composta por um único item e teve o propósito de investigar quais das ações de conscientização até agora realizadas foram, para o respondente, as mais interessantes, divertidas ou chamaram a sua atenção. Constatou-se que as ações que tiveram mais aceitação foram as referentes ao evento Serpro Security Week, principalmente as palestras, workshops e sala de escape. Nesta seção, os respondentes tinham a opção de acrescentar comentários sobre as ações, entre os que se destacam: “Nos instigava a ficar mais atentos” e “As ações realizadas ajudaram a destacar a importância do tema e mantê-lo no radar das equipes”.

Já sobre a engenharia social, procurou-se conhecer as atitudes dos empregados voltadas a minimizar a exposição a ataques de engenharia social. Observa-se que 50% dos empregados têm o hábito de comunicar ao setor responsável pela segurança, a presença de pessoa desconhecida e sem identificação, 56% não comentam assuntos relacionados ao Serpro em meios de transporte, bares, restaurantes ou redes sociais e quase 69% usam de forma correta o crachá. Verificou-se a existência de normativa do Serpro – a norma SG 002 – que trata do controle de acesso às instalações do Serpro. No que diz respeito à exposição de informações em locais externos, o Código de Ética do Serpro orienta os colaboradores a serem cautelosos com a divulgação de informações e documentos da empresa.

Quanto à senha segura observa-se que a ampla maioria dos empregados seguem as orientações de segurança recomendadas quanto à criação, guarda e digitação de

senhas. Assim, verifica-se que quase 94% dos participantes têm o hábito de desviar o olhar quando o colega digita a senha em sua estação de trabalho e 90% não emprestam a senha para colegas independentemente da gravidade da situação. Quase 72% dos respondentes, ao criar uma senha, afirmam que alternam números, letras e caracteres especiais, 65% não usam dados pessoais na sua composição e 59% verificam se alguém o está observando quando está digitando a sua senha. Existem duas normas do Serpro que tratam do assunto: a SG 018 que regulamenta a gestão de identidade e o controle de acesso lógico que deve ser aplicado às informações, sistemas e serviços corporativos do Serpro, visando a proteção dos ativos de informação contra o acesso não-autorizado e a SG 010 que disciplina as ações de segurança para o controle de contas de acesso, local e remoto, aos ambientes de tecnologia da informação e comunicação.

Os itens que compõem a seção “Sobre categorização da informação” foram criados no intuito de conhecer o grau de adesão dos colaboradores às boas práticas de preservação das informações sigilosas da empresa. Verifica-se que 65% dos respondentes protegem os documentos de trabalho de acesso não autorizado ou que contenham informações sigilosas, 56% conhecem os procedimentos e diretrizes sobre a categorização da informação do Serpro quanto ao grau de sigilo, 75% entendem que as informações sigilosas da empresa não podem ser compartilhadas com qualquer colega no ambiente de trabalho, 81% considera que não é apropriado comentar com familiares ou amigos próximos informações sigilosas às quais tenha acesso por conta do seu trabalho e 50% afirma que fragmenta os documentos que contêm informações sigilosas quando os descarta. A norma do Serpro que define os procedimentos de classificação, proteção e divulgação da informação sigilosa e as restrições de acesso, é a SG 005: Classificação dos ativos de informação do Serpro. De forma geral a SG 010, comentada na Seção “Sobre senha segura” ao regulamentar o controle de contas de acesso, também aborda a categorização das informações.

Constata-se a partir das respostas aos itens da seção “Sobre conexão segura” que o 62% dos respondentes têm o hábito de verificar se o site é seguro quando acessa

uma página da internet e quase 97% não realiza conexão de roteador WI-FI na sua estação de trabalho. Por outro lado observa-se que a prática de fazer teste com antivírus ao plugar uma mídia de origem desconhecida na estação de trabalho é realizada por 37% dos respondentes. O Serpro dispõe quatro normativas que contribuem para minimizar os riscos de segurança decorrentes de conexões na internet e de instalações de programas em equipamentos corporativos: a SG 013 que regulamenta os procedimentos sobre o uso de programas de computador nas estações de trabalho, a SG 008 que estabelece os critérios para utilização de acesso Web Internet e regulamenta os procedimentos para solicitar alteração nos sítios bloqueados, a SG 014 que regulamenta as ações a serem adotadas para a utilização segura dos serviços da intranet e internet e a SG 024 que regulamenta o acesso à Rede Serpro, incluindo os ambientes intranet e Internet, através de rede local sem fio (WLAN) do Serpro.

No que diz respeito à segurança na estação de trabalho a maioria dos respondentes demonstram um comportamento seguro. Assim, 53% dos participantes desligam o computador quando não está em uso, 81% bloqueiam a tela do seu computador cada vez que se afastam da sua estação de trabalho, 56% mantêm a mesa e estação de trabalho limpas e organizadas, quase 69% guarda em local seguro documentos com conteúdo de trabalho considerados sigilosos e 65% mantêm em local seguro os pen drives, HD e outras mídias que utiliza para o seu trabalho. Verifica-se que uma minoria tem o hábito de guardar o token em local seguro quando termina o expediente, sendo que 40,6% dos respondentes concordam totalmente com essa afirmativa. O uso seguro da estação de trabalho é regulamentado na norma SG 015.

No que diz respeito à segurança no recebimento de e-mails, nota-se que a prática de verificar a procedência de e-mails antes de abrir os anexos é bastante comum entre os respondentes, sendo que quase 94% deles concordam que procedem dessa forma. Nesta seção também é verificado que quase 72% dos empregados participantes descartam antes de abrir os e-mails de procedência duvidosa, 62% não utilizam o correio eletrônico corporativo para receber ou enviar mensagens pessoais

e 69% denunciam como spam ou bloqueiam o remetente quando recebem um e-mail com conteúdo tipo spam. A norma SG 016 regulamenta sobre o uso seguro de serviços institucionais de correio eletrônico e mensageria.

A seção que aborda a impressão segura de documentos foi constituída por um único item que questionou sobre o hábito de escolher um PIN da impressora diferente do padrão para imprimir documentos sigilosos. Nota-se que não existe um consenso entre os respondentes quanto a essa prática, sendo que 21,9% concordam totalmente, 18,8% concordam parcialmente, 31,3% não concordam nem discordam e 28,1% discordam. A norma do Serpro que obriga a utilização do PIN é a RE 008 que trata sobre o serviço de impressão corporativa.

A seção “Sobre meus conhecimentos em segurança da informação” objetivou constatar a percepção que têm os empregados quanto a seus conhecimentos e responsabilidades sobre segurança da informação. Verifica-se que 34% dos respondentes concordam totalmente que o conhecimento que eles detêm sobre o tema segurança da informação é suficiente para o desempenho das suas atividades, já o 50% concordam parcialmente com essa afirmativa. O conteúdo da política de segurança da informação do Serpro é conhecido pelo 12,5% dos respondentes, e o 75% concordam que o conhecem, mas de forma parcial. Quanto ao reconhecimento de sua responsabilidade pela proteção da informação que manuseia na empresa, a grande maioria admite que são responsáveis, sendo que 93,8% concordam totalmente com a afirmativa.

Por último, no intuito de ter embasamento para o planejamento de futuras ações, a pesquisa visou conhecer quais métodos são os preferidos dos empregados para adquirir conhecimentos sobre segurança da informação. Verifica-se que as palestras, workshops e minicursos são as metodologias de ensino favoritas entre todas as opções apresentadas.

4. CONSIDERAÇÕES FINAIS

As ações de conscientização têm como objetivo induzir as pessoas a prestar atenção sobre um determinado assunto. No ambiente corporativo, as ações de conscientização em segurança da informação são fundamentais considerando que a maior parte dos incidentes de segurança da informação ocorre por descuidos ou desconhecimento das pessoas. Por isso, a norma ISO 27002, orienta a que todos os colaboradores da organização recebam treinamento, educação e conscientização apropriados, e atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções.

Esta pesquisa demonstra que a empresa em estudo possui um arcabouço de normativas, separadas por temas, que fundamentam a sua política de segurança da informação. E nesse contexto, as ações de conscientização analisadas tiveram como foco disseminar o conteúdo dessa política, além de fomentar a adesão às melhores práticas de segurança da informação.

Percebe-se que as ações foram direcionadas a todos os empregados, independentemente do seu cargo e lotação, no intuito de tornar as normas compreensíveis para todos os públicos. Por isso, utilizaram-se múltiplos canais, como é recomendado pela norma ISO 27002. Constatou-se que entre todas as ações realizadas, as palestras, os workshops e a sala de escape foram as mais votadas pelos participantes, indicando-as como as ações mais interessantes, divertidas ou as que chamaram mais a sua atenção.

Verifica-se, por meio da análise das respostas aos itens, que a maioria dos respondentes está aderente às boas práticas de segurança da informação. Todavia, a realização de teste com antivírus ao plugar uma mídia de origem desconhecida, o hábito de guardar o token em local seguro quando termina o expediente e a escolha de um PIN da impressora diferente do padrão para imprimir documentos sigilosos são práticas que ainda não estão consolidadas. Além disso, existe uma parcela importante dos respondentes que não conhece de forma integral o conteúdo da

política de segurança da informação da empresa. Essas lacunas confirmam a necessidade de futuras ações de conscientização as quais poderão se fundamentar nos resultados desta pesquisa, direcionando os esforços para os itens que apresentaram menor concordância com boas práticas de segurança da informação.

Quanto à modalidade de ensino que os empregados preferem para assimilação de conteúdo sobre segurança da informação, o resultado da pesquisa aponta que são as palestras, workshops e minicursos. Esta informação é importante na medida em que poderá ser utilizada para o planejamento de futuras ações, inclusive, de outras empresas que desejem implementar um programa de conscientização em segurança da informação.

Assim, a partir dos resultados expostos conclui-se que as ações de conscientização são fundamentais tanto para internalizar a política de segurança da informação de uma empresa como para promover o comportamento seguro dos colaboradores.

REFERÊNCIAS

ARAÚJO, Pedro Henrique de Moura. **Construção da escala do nível da cultura organizacional de segurança da informação**. Orientador: Dalton Francisco de Andrade. 2018. 205 f. Tese (Doutorado em Engenharia de Produção) – Universidade Federal de Santa Catarina, Florianópolis, 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ABNT NBR ISO/IEC 27001**: tecnologia da informação: técnicas de segurança: sistemas de gestão de segurança da informação: Requisitos. Rio de Janeiro: ABNT, 2013a.

_____. **ABNT NBR ISO/IEC 27002**: tecnologia da informação: técnicas de segurança: código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2013b.

AXELOS. **Glossário e abreviações ITIL**. 2011. Versão 1.0. London: Axelos, 2011.
Disponível em:

RC: 98717

Disponível em: <https://www.nucleodoconhecimento.com.br/administracao/acoes-de-conscientizacao>

https://www.axelos.com/Corporate/media/Files/Glossaries/ITIL_2011_Glossary_BR-PT-v1-0.pdf. Acesso em: 13 abr.2020.

BRASIL. Tribunal de Contas da União. **Boas práticas em segurança da informação**. 4. ed. Brasília, DF: Tribunal de Contas da União, 2012. 103 p.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.BR). **Cartilha de segurança para internet**. [São Paulo: Comitê Gestor da Internet no Brasil], 2018. Disponível em: <http://cartilha.cert.br/>. Acesso em: 2 abr.2020.

COELHO, Flávia Estéla Silva; ARAÚJO, Luiz Geraldo Segadas de. **Gestão da segurança da informação**: NBR 27001 e 27002. Rio de Janeiro: Escola Superior de Redes, 2013. 193 p. ISBN 978-85-63630-12-4.

CUNHA, Roberto. **Treinando macacos, educando pessoas**: segurança da informação se faz com tecnologia, processos e pessoas, e a formação destas exige mais que uma sequência de treinamentos: porque você treina macacos: pessoas, você educa. Orientador: André Valle. 57 f. Trabalho de Conclusão de Curso (Especialização em Gerência de Telecomunicações) – Fundação Getúlio Vargas, Belo Horizonte, 2007.

DANTAS, Marcus Leal. **Segurança da Informação**: uma abordagem focada em gestão de riscos. Olinda: Livro Rápido, 2011. 150 p. ISBN 978-85-406-0047-8.

DOURADO, Luzia Moreira de Abreu; ALVES, André Luiz. **Um estudo sobre os habilitadores do COBIT® 5 sob a perspectiva da segurança da informação**. 2016. [18] f. Artigo (Grau em Curso) – Pontifícia Universidade Católica de Goiás, Goiânia, 2016.

FONSECA, Paula Fernanda. **Gestão de segurança da informação**: o fator humano. 2009. [16] f. Artigo (Especialização em Redes e Segurança de Computadores) – Pontifícia Universidade Católica do Paraná, Curitiba, 2009.

RC: 98717

Disponível em: <https://www.nucleodoconhecimento.com.br/administracao/acoes-de-conscientizacao>

FONTES, Edison Luiz Gonçalves. **Políticas de segurança da informação**. Rio de Janeiro: Escola Superior de Redes, 2015. 114 p. ISBN 978-85-63630-37-7.

IT GOVERNANCE INSTITUTE. **COBIT 4.1**: modelo, objetivos de controle, diretrizes de gerenciamento, modelos de maturidade. Rolling Meadows, IL: IT Governance Institute, c2007. 200 p.

PORTAL GSTI. **O que é ISO 27001 e 27002?** [S. l.]: Portal GSTI, c2020. Disponível em: <https://www.portalgsti.com.br/iso-27001-iso-27002/sobre/>. Acesso em: 20 abr.2020.

RIOS, Orlivaldo Kléber Lima; RIOS, Vânia Patrícia da Silva; TEIXEIRA FILHO, José Gilson de Almeida. Melhores práticas do COBIT, ITIL e ISO/IEC 27002 para implantação de política de segurança da informação em instituições federais do ensino superior. **Gestão & Tecnologia**, Pedro Leopoldo, v. 17, n. 1, p. 130-153, jan./abr. 2017.

UNIVERSIDADE DE BRASÍLIA. Faculdade de Ciência da Informação (Ed.). **Gestão da segurança da informação e comunicações**. Brasília, DF: Faculdade de Ciência da Informação, 2010. 121 p. (Série segurança da informação, v. 1).

WILSON, Mark; HASH, Joan. **Building an information technology security awareness and training program**: computer security. Gaithersburg, MD: National Institute of Standards and Technology, 2003. 39 p. Publicação especial NIST 800-50.

WUNSCH, Ademir. **Modelo de governança de TI para uma indústria metalúrgica**. Orientadora: Ângela Freitag Brodbeck. 2010. 73 f. Trabalho de Conclusão de Curso (Especialização em Administração da Tecnologia da Informação) – Universidade do Vale do Rio dos Sinos, São Leopoldo, 2010.

ANEXO I

Itens do questionário e gráficos das respostas

RC: 98717

Disponível em: <https://www.nucleodoconhecimento.com.br/administracao/acoes-de-conscientizacao>

SOBRE AS AÇÕES DE CONSCIENTIZAÇÃO REALIZADAS NO PERÍODO DE 2016 A 2020

Marque as opções que foram interessantes, divertidas ou chamaram sua atenção.

32 respostas

SOBRE ENGENHARIA SOCIAL

Comunico ao setor responsável pela segurança quando percebo a presença de pessoa desconhecida e que não esteja utilizando identificação nas instalações da Regional Florianópolis.

32 respostas

Comento assuntos relacionados ao Serpro em meios de transporte, bares, restaurantes ou redes sociais.

32 respostas

Eu sempre utilizo o meu crachá de identificação em local visível quando estou nas instalações da empresa.

32 respostas

SOBRE SENHA SEGURA

Tenho o hábito de desviar o olhar quando meu colega digita a senha em sua estação de trabalho.

32 respostas

Não empresto minha senha para colegas independentemente da gravidade da situação.

32 respostas

Ao criar uma senha alterno números, letras e caracteres especiais.

32 respostas

Quando crio uma senha não utilizo dados pessoais.

32 respostas

Verifico se alguém está me observando quando estou digitando minha senha.

32 respostas

SOBRE CATEGORIZAÇÃO DA INFORMAÇÃO

Eu protejo os documentos de trabalho de acesso não autorizado ou que contenham informações sigilosas.

32 respostas

Eu conheço os procedimentos e diretrizes sobre a categorização da informação do Serpro quanto ao grau de sigilo.

32 respostas

Entendo que informações sigilosas da empresa podem ser compartilhadas com qualquer colega no ambiente de trabalho.

32 respostas

Considero comum comentar com familiares ou amigos próximos informações sigilosas às quais tenho acesso por conta do meu trabalho.

32 respostas

Eu fragmento os documentos que contêm informações sigilosas quando vou descartá-los.

32 respostas

SOBRE CONEXÃO SEGURA

Verifico se o site é seguro quando acesso uma página da internet.

32 respostas

Faço ou peço para fazer teste com antivírus ao plugar uma mídia de origem desconhecida na minha estação de trabalho (pen drive, HD externo ou outras mídias).

32 respostas

Faço conexão de roteador WI-FI na minha estação de trabalho, no ambiente físico da empresa.

32 respostas

SOBRE SEGURANÇA NA ESTAÇÃO DE TRABALHO

Eu desligo o meu computador quando não está em uso.

32 respostas

Bloqueio a tela do meu computador cada vez que me afasto da minha estação de trabalho.

32 respostas

Mantenho a minha mesa e estação de trabalho limpas e organizadas.

32 respostas

Guardo em local seguro documentos com conteúdo de trabalho considerados sigilosos.

32 respostas

Mantenho em local seguro pen drive, HD e outras mídias que utilizo para o meu trabalho.

32 respostas

Guardo o token em local seguro quando termina meu expediente.

32 respostas

SOBRE SEGURANÇA NO RECEBIMENTO DE E-MAILS

Verifico a procedência dos e-mails antes de abrir os arquivos anexos.

32 respostas

Eu descarto sem abrir os e-mails de procedência duvidosa.

32 respostas

Utilizo o correio eletrônico corporativo para receber ou enviar mensagens pessoais.

32 respostas

Denuncio como spam ou bloqueio o remetente quando recebo um e-mail com conteúdos tipo spam (propagandas, anúncios...)

32 respostas

SOBRE SEGURANÇA NA IMPRESSÃO DE DOCUMENTOS

Escolho um PIN da impressora diferente do padrão para imprimir documentos sigilosos quando estou no ambiente físico da empresa.

32 respostas

SOBRE MEUS CONHECIMENTOS EM SEGURANÇA DA INFORMAÇÃO

Meu conhecimento sobre o tema segurança da informação é suficiente para o desempenho das minhas atividades.

32 respostas

Eu conheço o conteúdo da política de segurança da informação do Serpro.

32 respostas

Reconheço minha responsabilidade pela proteção da informação que manuseio no Serpro.

32 respostas

SOBRE OS MEIOS DE CONSCIENTIZAÇÃO PARA AÇÕES FUTURAS

Assinale as opções de sua preferência para aprender mais sobre segurança da informação.

32 respostas

Enviado: Fevereiro, 2021.

Aprovado: Outubro, 2021.