Campanha de Conscientização em Segurança da Informação: Um Estudo de Caso

Rodrigo Costa dos Santos
prof.rodrigo.santos@gmail.com
COPPE/UFRJ

Manuela Fernandes dos Santos
manufernandessantos@live.com
UNESA

Fernando Spencer Carreira
fspencer@gmail.com
IBMEC-RJ

Resumo: Este artigo tem por objetivo apresentar os resultados de um estudo de caso sobre os efeitos e benefícios de uma campanha de conscientização em segurança da informação numa empresa do setor elétrico brasileiro. A campanha foi realizada no período de uma semana, após criação da Política de Segurança da Informação desta empresa, além disso, contou com ações voltadas para diverso públicos: estratégico, tático e operacional. A campanha foi tratada como um projeto, seguindo o PMBOK (Guia de Gerenciamento de Projetos do PMI), sendo estabelecido um líder, patrocinador e partes interessadas, bem como o controle de tempo, custos e recursos necessários, sendo esse um dos motivos do sucesso da campanha. Este estudo de caso foi realizado com base na análise da pesquisa de satisfação dos colaboradores participantes. Os principais resultados apontam que a campanha atingiu a expectativa dos colaboradores, que os temas tratados foram relevantes ao cotidiano da empresa e os materiais utilizados e palestrantes contribuíram muito para a aderência e disseminação do conhecimento. Os colaboradores contribuíram com sugestões de tema para próximas campanhas, que, após o sucesso desta, foi sugerida a realização de novas campanhas anuais, realizadas sempre no mês de novembro, tornando este, o mês da Segurança da Informação nesta empresa.

Palavras Chave: Segurança Informação - Conscientização - Política Segurança - Norma ISO 27002 - Gestão de Pessoas

1. Introdução

Segurança da Informação pode ser definida como a área do conhecimento dedicada à proteção de ativos de informação contra acessos e alterações indevidas de forma a garantir a confiabilidade, integridade e disponibilidade das informações (SÊMOLA, 2004).

Por muito tempo a segurança da informação era tratada apenas tecnicamente, com proteção de documentos em papel e redes de dados, como uso de antivírus, firewall e outras ferramentas similares. Porém, ultimamente, muito se fala em espionagem, privacidade, engenharia social, que são temas que se faz repensar a oportunidade de avaliar de que forma empresas e empregados estão contribuindo para que informações estratégicas e sigilosas vazem ao mercado.

A literatura a cerca da Segurança da Informação indica que a criação da Política de Segurança é sempre um dos primeiros passos para se implantar um sistema de gestão de segurança da informação (ISO 27001, 2013). Contudo, somente a criação da Política não é o bastante, pois o fator humano deve ser considerado, pois são as pessoas que devem cumprir a política estabelecida. Nesse sentido, as campanhas de conscientização são a ferramenta mais apropriada para engajar as pessoas e garantir que estas recebam treinamento, educação e conscientização apropriados em consonância com as políticas e procedimentos organizacionais.

O presente artigo apresenta um estudo de caso da implantação de uma campanha de conscientização em segurança da informação em uma empresa do setor de energia, evidenciando as ações realizadas, todo seu público alvo e as avaliações e resultados alcançados. Para tanto, além desta introdução, o artigo possui um capítulo que faz a revisão da literatura, outro para o desenvolvimento do tema, seguidos pelo estudo de caso, resultados e finalizando com as conclusões.

2. Revisão da Literatura

Segundo o NIST (1998), a conscientização é o catalizador que, por meio de uma informação sobre um determinado assunto, alguém passa a prestar atenção (tomar conhecimento, se conscientizar) sobre um problema, possibilidade, entre outro tema. Por isso é correto afirmar que a conscientização dentro das organizações é de suma importância, ainda mais quando se trata de Segurança da Informação, pois os colaboradores ainda não tem a noção das reais ameaças que põe as informações organizacionais em risco.

É importante salientar que no atual ambiente competitivo todos os colaboradores devem ser conscientizados. Segundo a ISO 27002 (2013), convém que todos os colaboradores da organização recebam treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções. De acordo com a NIST 800-16 (1998) a conscientização de segurança é obrigatória para todos os colaboradores, incluindo empregados, contratados, estagiários e quem está envolvido de alguma forma com sistemas de TI.

Por isso pessoas que realizam trabalho sob o controle da organização devem estar cientes da política de segurança da informação, suas contribuições para a eficácia do sistema de gestão da segurança da informação, incluindo, os benefícios da melhoria do desempenho da segurança da informação, e implicações da não conformidade com os requisitos do sistema de gestão da segurança da informação (ISO 27001, 2013).

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 (NIST 800-16,1998).

Para o desenvolvimento de uma campanha de conscientização, é importante seguir alguns passos a fim de alcançar os resultados esperados. O primeiro passo é a escolha da equipe responsável pelo desenvolvimento, realização e manutenção do programa. Segundo a PCI (2014), é recomendado que a equipe seja formada com pessoal de diferentes áreas de atuação, com diferentes responsabilidades dentro da empresa. Ter esta equipe dentro da empresa garante o sucesso do Programa. O número de membros depende de necessidades específicas de cada organização e de sua cultura.

O segundo passo se refere à seleção do público da conscientização, o ideal é agrupar os indivíduos de acordo com suas funções dentro da empresa. O nome dado a este tipo de conscientização é Programa de Conscientização baseado em funções. Pode-se dividir este público em três funções: todo o pessoal, especialistas e gerentes.

Na função “Todo o pessoal”, o programa irá ajudar a reconhecer ameaças, enxergar a segurança como benéfico o suficiente para transformar num hábito no trabalho e em casa, e sentir confortável reportando problemas de segurança, como vírus, spam, worms, etc.

Na função “Especialista”, o programa irá focar na obrigação individual para seguir procedimentos seguros na manipulação de informações sensíveis e reconhecer os riscos associados se o acesso privilegiado é roubado. Cada um dos especialistas necessita de treinamento e conscientização para construir e manter um ambiente seguro.

Na função “Gerentes”, o programa pode diferenciar dos outros dois tipos. Eles precisam entender a política de segurança da organização e os requisitos de segurança o suficiente para discutir e reforçar a mensagem para os colaboradores, encorajando a conscientização dos colaboradores, no momento de reconhecer e relatar quando um problema de segurança ocorrer. O nível de conscientização dos gerentes pode precisar também de incluir uma compreensão geral de como as diferentes áreas se encaixam. Gerentes com acesso privilegiado deve ter um entendimento sólido de requisitos de segurança dos seus colaboradores, especialmente aqueles com acesso a dados sensíveis. O treinamento de gerentes ajudará nas decisões sobre proteção da Informação da Organização.

Independentemente da função, é recomendado que todos os colaboradores recebam treinamento básico de conscientização de segurança, desenvolvido em concordância com as políticas de segurança organizacional.

Após a definição dos grupos a serem conscientizados, há a necessidade da segmentação de material de divulgação adequado para cada público em tempo hábil e eficiente. Segundo a NIST 800-50 (2003), para ser eficaz, o canal de comunicação deve se encaixar na cultura organizacional. Disseminando o programa através de múltiplos canais, a empresa garante que os colaboradores estarão expostos às mesmas informações múltiplas vezes de formas diversas. O canal de comunicação usado e o seu conteúdo, deve coincidir com o público da conscientização.

Quanto ao conteúdo, existe um vasto número de temas que podem ser abordados, por isso de acordo com a NIST 800-50 (2003), um número significante de assuntos podem ser mencionados e facilmente discutidos numa campanha: uso e gerenciamento de senha, incluindo criação, frequência de troca e proteção; proteção contra vírus, worms, cavalos de troia e outros códigos maliciosos; políticas (implicações do não cumprimento); e-mails e anexos desconhecidos; uso da Web (liberação versus proibição, monitoramento das atividades de usuários); spam; backup de dados e armazenamento (abordagem centralizada ou descentralizada); engenharia social; resposta a incidentes (Quem devo contatar? O que eu faço?); mudanças no ambiente do sistema (aumento dos riscos para o sistema e para os dados: água, fogo, seco ou molhado, acesso físico); inventário e transferência de propriedade (Identificar a Organização responsável e as responsabilidades dos usuários); uso pessoal e questões de ganho (sistemas no trabalho e em casa); questões de segurança em dispositivos portáteis (identificar tanto questões físicas quanto segurança do wireless); uso de criptografia e transmissão de informações sensíveis/ confidenciais através da internet (identificar políticas, procedimentos e contato técnico pra assistência); segurança de computador durante viagens (identificar tanto questões de segurança física quanto de segurança da informação); sistemas e software de propriedade pessoal no trabalho (indicar se é permitido ou não); licenças de software (identificar quando cópias são permitidas ou não); controle de acesso (identificar lista de privilégios); responsabilidade individual (explicar o que isso significa na Organização); uso de declarações de confirmação (senhas, acesso a sistemas e dados, uso e ganho pessoal); controle de visitantes e acesso físico aos espaços (discutir política de segurança física aplicável e procedimentos, relatórios de atividades fora do comum); segurança da área de trabalho. Independente do conteúdo e método utilizado, os materiais de treinamento devem estar disponíveis para todas as áreas da organização (PCI, 2014).

Diante de tantos possíveis assuntos para uma campanha, é necessário levar em conta as formas de aprendizado de cada colaborador. Tudo isso porque alguns teóricos da área de pedagogia, explicam que cada indivíduo aprende de uma forma, por isso algumas teorias foram desenvolvidas. São várias as teorias de estilo de aprendizagem, mas, a mais difundida é a Teoria do pesquisador em Neurolinguística Walter Barbe, onde ele defende três estilos: visual, auditivo e cinestésico. Para ele o estilo visual é aquele baseado em leitura, vídeo-aulas, filmes, gráficos, tabelas. O estilo auditivo é através de palestras, seminários e recursos de áudio. E o estilo cinestésico precisa de experiências práticas, como estudos de caso, atividades em laboratório, dinâmica em grupo.

Com base nesta teoria, além de nos atentarmos para a forma de aprendizagem, se faz necessária a utilização de diferentes recursos a fim de facilitar a aderência de cada indivíduo. Elas podem ser: ferramentas de conscientização (canetas, chaveiros, post-it,

blocos de anotação, kits de primeiros socorros, marcadores de texto, frisbees, relógios); pôster "O que fazer e o que não fazer", ou checklist; fundo de tela; newsletters; alertas na intranet; e-mails; vídeos; cursos no computador; curso na internet; teleconferência; palestras; Dia da Segurança de TI ou eventos parecidos; coffee break; pop-up com informações de segurança da informação e dicas mensais; quebra-cabeça; cartilhas.

Ao citar cartilhas, tem-se como referência as cartilhas desenvolvidas pelo CERT.Br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil) que é o responsável pelo tratamento de incidentes de segurança em computadores que envolvam redes conectadas à internet brasileira. Além do processo de tratamento a incidentes, o CERT.br também atua através do trabalho de conscientização sobre os problemas de segurança, da análise de tendências e correlações entre eventos na Internet Brasileira e do auxílio ao estabelecimento de novos CSRITs (Grupo de Segurança e Resposta a Incidentes) no Brasil. Em seu site www.cartilha.cert.br, são disponibilizadas informações atualizadas sobre ameaças, golpes e prevenção dos usuários.

3. Desenvolvimento

Estamos na Era da Informação, o que significa uma maior disseminação da informação, em tempo real e a utilização da tecnologia para sua geração e transmissão. Numa organização, a informação é um dos ativos mais importantes, e por isso, um dos maiores desafios das organizações, é a proteção destas informações, a prevenção contra ameaças e a conscientização dos seus colaboradores. De acordo com Alimaqousi, Balikhina e Mackay (2013), uma das ameaças mais significantes para segurança da informação são os usuários de sistemas, porque eles estão familiarizados com a infraestrutura e serviços, mas eles podem não estar conscientizados sobre as políticas de segurança, seu significado e seu papel na proteção dos dados.

O foco dos analistas de segurança da informação tem sido a proteção, o monitoramento, e o grande equívoco disso tudo, é empenhar seus esforços quase que exclusivamente, na adoção de recursos tecnológicos avançados. Segundo Luiz Guelman (2006), de nada adianta investir em tecnologia e proteção física se não se tem a colaboração e o comprometimento das pessoas. Conforme Krueger, Drevin e Stetyn (2008), regularmente grandes quantias de dinheiro e tempo são investidos por Organizações em soluções técnicas para assuntos de segurança enquanto o fator humano recebe menor atenção. Soluções técnicas são claramente necessárias para identificar vulnerabilidades como vírus, evitar ataques, e prevenir acesso não autorizado.

Fabricio Basto (2015) argumenta que pesquisas recentes revelam que a maioria dos incidentes de segurança são ocasionados no ambiente interno, sendo que atualmente a grande parte dos recursos são investidos no ambiente externo (medidas de proteção, firewall, IDS, etc.). Seria fácil se isso fosse o suficiente para alcançar o objetivo pretendido, mas a equipe interna pode ser um grande problema, se não for bem treinada.

Pois os sistemas são operados por pessoas, o elo mais fraco desta história, que na maioria das vezes não estão preparados para lidar com as ameaças diárias, como invasão do sistema, vazamento de informações sigilosas, etc. Gross e Rosson (2007), tem o mesmo ponto de vista sobre o fator humano. Ele também defende a ideia de que o usuário é o elo fraco referente à segurança da informação, e que um único usuário pode colocar toda a organização em perigo. E ainda segundo Luiz Guelman (2006), nas organizações, a grande maioria dos empregados tem uma falsa sensação de segurança, principalmente quando estão utilizando recursos de informática, pois sabem que existem profissionais dedicados e softwares de segurança atualizados e se sentem de alguma forma protegidos.

Muitos analistas preferem simplesmente bloquear o acesso à internet, bloquear o acesso à rede corporativa, mas o recomendável é a elaboração de um programa de conscientização, onde todos da organização, desde a alta administração aos usuários finais, sejam conscientizados quanto à correta utilização dos recursos tecnológicos, as consequências do mau uso, tanto para o indivíduo quanto para a organização. Este programa deve ter uma regularidade, no mínimo anual, para que informações não retidas anteriormente sejam revistas e novas informações adquiridas.

O material a ser utilizado no programa deve ser elaborado pensando no público a ser alcançado, visto que o programa visa atender todos da organização. Segundo a PCI (2014), a chave para um programa de conscientização de segurança eficaz é a segmentação de material relevante para o público adequado em tempo hábil e eficiente. Para ser eficaz, o canal de comunicação deve também se encaixar na cultura organizacional. Disseminando o treinamento através de múltiplos canais, a organização assegura que o pessoal estará exposto à mesma informação múltiplas vezes de diferentes formas.

O conteúdo pode precisar ser adaptado dependendo do canal de comunicação, por exemplo, o conteúdo num boletim eletrônico pode ser diferente de um conteúdo de um seminário de treinamento, mesmo assim as duas formas tem a mesma mensagem. Para isso é necessário uma pré-avaliação, com a finalidade de avaliar o grau de conhecimento dos usuários e suas reais necessidades, quanto a estas ameaças e riscos já citados.

Nas organizações que já estabeleceram seu programa, em sua grande maioria, não houve a preocupação de avaliar o conhecimento do participante, e desta forma elaborar um material e estratégia adequados para o público alvo. Este tipo de evento deve ocorrer depois de certo tipo de maturidade dos colaboradores quantos aos assuntos pertinentes ao tema de segurança da informação. E o principal objetivo deve ser conscientizar sobre o porquê deste evento. Antes disso, devem-se criar métricas, e indicadores, como forma de avaliar a percepção do colaborador quanto aos temas e sua aderência. Deve ser feita antes e depois do evento. Antes para definir o nível de cada colaborador. E depois para descobrir quanto absorveu.

Em vista de todos estes argumentos, em 2012, após a elaboração da Política de SIC numa empresa do setor elétrico, foi estudada a criação de uma campanha anual de conscientização sobre segurança de TI, onde seriam utilizados diversos materiais e seriam abordados temas relevantes contemplados na política da empresa. Neste trabalho, será abordado um estudo de caso realizado nesta empresa do setor elétrico.

4. Estudo de caso

Segundo Robert Yin (2015) em seu livro "Estudo de Caso - Planejamento e Métodos", um estudo de caso investiga um fenômeno contemporâneo (o caso) em seu contexto no mundo real, especialmente quando as fronteiras entre o fenômeno e o contexto puderem não estar claramente evidentes. Este método responde as perguntas "como" e "por que".

Por isso, foi escolhido este método de pesquisa qualitativa, onde, após realização dos eventos dentro da empresa, foi realizada uma pesquisa de satisfação, a qual os respondentes eram os participantes dos eventos, avaliando as atividades desenvolvidas, os palestrantes, os recursos utilizados e o conteúdo ministrado.

O evento em questão, ora apresentado nesse artigo, trata-se da 1ª Semana de Conscientização em Segurança da Tecnologia da Informação de uma grande empresa do setor de energia elétrica. Essa Semana de Conscientização de SI foi tratada como um projeto dentro da companhia, seguindo a metodologia de Gerenciamento de Projetos, com base no guia PMBOK (PMI, 2015), o qual orienta a indicação de um líder para o projeto e demais partes interessadas, como patrocinador, gestor de projeto e coordenador de comunicação. Para determinar os prazos para cada atividade, foi elaborado um cronograma. E ainda fazendo uso desta metodologia, pudemos estimar os custos, recursos, premissas e restrições do projeto. Essa formalização em Projeto foi fundamental para o sucesso da campanha, pois conseguimos garantir a execução das atividades dentro do escopo, do custo e prazo; além de garantir a qualidade dos produtos entregues, garantir a satisfação dos *stakeholders*; controlar os problemas e riscos do projeto e gerar lições aprendidas para as próximas campanhas.

Por isso este estudo de caso visa expor os resultados desta campanha de conscientização de SI realizada pela Divisão de Segurança de TIC de uma empresa do setor elétrico, que teve como objetivo a conscientização e educação dos usuários e colaboradores desta empresa sobre a Política de Segurança de TIC, implementada pela primeira vez na empresa. Esta política de segurança apresenta várias diretrizes, dentre elas, destacam-se:

> *I - Deve ser assegurado pela empresa que esta política e suas normas complementares* ***estejam amplamente divulgadas aos seus colaboradores****, visando a sua disponibilidade para todos que se relacionam com a organização e que, direta ou indiretamente são impactados.*
>
> *II - Deve ser assegurado pela empresa que as alterações desta política e de suas normas complementares* ***sejam devidamente comunicadas aos seus colaboradores****. Todavia, deve ser esclarecido que é responsabilidade de cada colaborador a consulta esporádica e voluntária para identificar possíveis atualizações dos instrumentos.*
>
> *III - A empresa deve* ***possuir um Plano Anual de Conscientização em Segurança da Informação visando à capacitação e disseminação a cultura de Segurança da informação junto aos seus colaboradores*** *em relação ao uso ético, seguro e legal das novas tecnologias e ferramentas de trabalho, bem como das informações e recursos disponibilizados.*

Portanto, baseando-se nestas diretrizes, como escopo do projeto, foram elaboradas 7 (sete) ações de conscientização diferentes e para públicos diferentes. Os públicos-alvo foram separados em 3 (três) categorias: Estratégico, Tático e Operacional, conforme figura 1. O público estratégico compreende o presidente, os diretores e demais alto executivos da companhia. O público tático é formado pelos chefes de departamento e divisão, além dos coordenadores de equipe e líderes de projeto. O público operacional compreende todos os funcionários da empresa não gerentes, técnicos, estagiários, incluindo os prestadores de serviço da companhia.

Figura 1: Categoria dos públicos-alvo (*dos autores*)

A separação dos públicos–alvo se faz necessária para maximizar o nível de assimilação das ações de conscientização, pois, dependendo do público, há diferença na forma com que cada um está exposto às informações sensíveis da companhia, e isso acarreta na diferença em quais pontos da política de segurança da informação deverão ser abordados. Além disso, existe uma diferença entre a linguagem e a forma de tratar a informação com cada público desses. Adicionalmente, a diversidade das ações também leva em conta o meio de comunicação utilizado, por exemplo, muitos prestadores de serviços não possuem acesso a um computador e, nesse caso, as ações como palestras, cartazes e filmes se justificam, pois abrange uma categoria de colaboradores que não possuem acesso ao computador corporativo.

Contudo, cabe ressaltar que todas as ações estavam disponíveis para todos os colaboradores da empresa, sem restrições, porém cada ação foi concebida tendo como foco principal seu público-alvo prioritário.

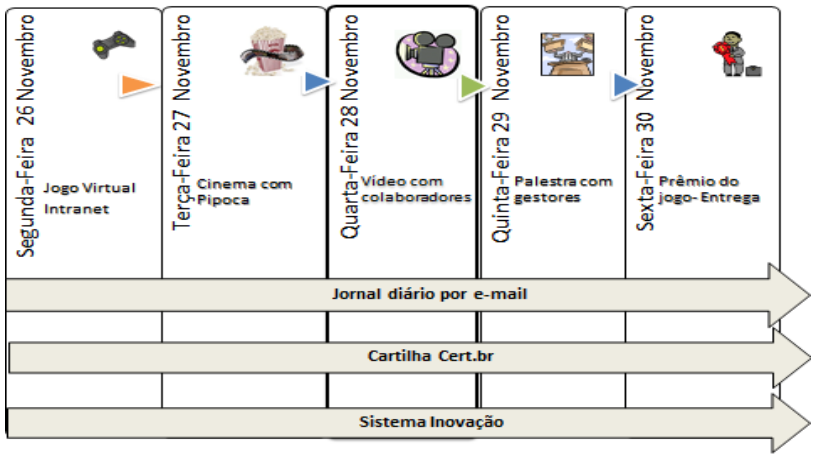


Figura 2: Programação da campanha

A programação da campanha de segurança é apresentada na figura 2 e as sete ações estão detalhadas a seguir:

1. **Vídeo com os empregados na Intranet** expondo situações cotidianas sobre o tema. Público-alvo prioritário: Tático e operacional.

Elaboração de vídeo com situações ligadas ao cotidiano da empresa ligadas à Segurança da Informação. A filmagem foi realizada com os próprios colaboradores da empresa com apoio da área de comunicação corporativa, o que gerou internamente uma grande repercussão entre os colaboradores. O vídeo retrata 4 (quatro) situações:

a) Bloqueio do computador na ausência da estação de trabalho.

Nesta cena um colaborador ausenta-se de sua estação e não bloqueia o computador. Ao mesmo tempo um entregador (pessoa externa à companhia), que estava no local, visualiza o projeto da nova logomarca da empresa antes de torna-la pública à sociedade.

b) Impressão de documentos confidenciais

Nesta cena a secretária envia documentos confidenciais para impressão, mas, ocorre uma demora na busca destes documentos na impressora. Outro colaborador, ao retirar seu documento da impressora, teve acesso ao documento confidencial enviado pela secretária e os leva consigo. A secretária ao chegar na impressora entra em pânico ao reparar que os documentos não estavam lá.

c) Conversas em elevadores, corredores, táxis e locais públicos

Nesta cena dois colaboradores conversam sobre um projeto sigiloso que ainda não pode ser apresentado à mídia dentro do elevador da empresa, e não percebem que há outros colaboradores, inclusive um prestando atenção e possivelmente divulgando para outros colaboradores ou pessoas externas via celular.

d) Login e senha são pessoais e intransferíveis

Nesta cena um gerente liga de fora da empresa e informa seu login e senha para um funcionário e solicita que realize alguma atividade com seus dados. Depois disso, o colaborador, tendo a posse do login e senha do gerente, aproveita para abonar suas faltas no sistema.

2. **Jogo virtual on-line na Intranet**
Público-alvo prioritário: Operacional.

Jogo virtual denominado "Corrida da informação", em formato de tabuleiro, disponibilizado via intranet para todos os colaboradores, conforme tela demonstrada na figura 3. O avanço nas casas é condicionado a respostas corretas de perguntas ligadas a Segurança da Informação e extraídas da Política de Segurança da Informação e das normas específicas da empresa. O usuário é identificado automaticamente no início do jogo e a pontuação é gravada em registro de log. Cada colaborar podia jogar quantas vezes quisesse durante a semana.

Figura 3: Telas do jogo virtual "Corrida da Informação"

3. **Palestras de Conscientização com o *Gen. General Marconi dos Reis Bezerra - DSIC e Dra. Patrícia Peck Pinheiro – PPP***
Público-alvo prioritário: Estratégico e tático.

O General Marconi dos Reis Bezerra possui formação de Oficial do Exército e graduado em Engenharia de Telecomunicações pelo Instituo Militar de Engenharia. Ele é o Diretor da DSIC-Departamento de Segurança da Informação e Comunicações-da Casa Militar da Presidência da República, onde algumas de suas missões são a de orientar a implementação de ações de segurança da informação e comunicação, inclusive segurança cibernética no âmbito da administração pública federal. Sua palestra teve como tema "Segurança da Informação e Comunicações na Administração Pública Federal". O General demonstrou a evolução das Políticas de Segurança da Informação e Comunicação através de uma linha do tempo; alguns ataques ocorridos no Brasil e como se proteger.

A Prof. Dra. Patricia Peck Pinheiro é advogada especialista em Direito Digital formada pela USP, com especialização em negócios pela Harvard Business School,

curso de Gestão de Riscos pela Fundação Dom Cabral e MBA em marketing pela Madia Marketing School. Além disso, possui vasta experiência no campo do direito digital e investigação forense de crimes digitais. Sua palestra teve como tema "Conscientização em Segurança da Informação". Ela falou sobre uso e postura nas redes sociais, termos de uso destas redes, BYOD - *Bring Your Own Device* – (dispositivos móveis no ambiente de trabalho), riscos digitais, Lei Carolina Dieckmann, liberdade de expressão, vazamento de informações, direitos autorais.

4. **Dicas no jornal diário enviado por e-mail.**
Público-alvo prioritário: Tático e operacional.

Informativos enviados diariamente para e-mail corporativo de todos os colaboradores durante toda semana de Segurança da Informação. Abaixo destaca-se dois informes de dois dias diferentes:

"Semana de Segurança da Informação
30 de novembro é o Dia Internacional da Segurança da Informação e, para marcar essa data, a Empresa organiza sua primeira Semana Interna de Segurança da Informação. De hoje até a próxima sexta-feira, a empresa promoverá diversas ações com o objetivo de conscientizar os usuários e divulgar a Política de Segurança de TIC, aprovada em Diretoria Executiva. Dentre as ações previstas, estão a divulgação de dicas de segurança da informação e um jogo virtual com perguntas sobre o tema, que premiará os colaboradores que atingirem as maiores pontuações. O vídeo da semana na TV corporativa também aborda este assunto. Confira aqui."

"Segurança da Informação
O Departamento de Tecnologia da Informação recomenda que, ao imprimir um documento confidencial, o colaborador busque-o imediatamente na impressora. Deixar para buscá-lo depois possibilita que alguém tenha acesso a ele antes de você. Hoje, último dia da Semana de Segurança da Informação, será publicado na intranet, às 18h, o resultado do jogo virtual. Os vencedores retirarão seus brindes a partir da segunda-feira."

5. **Cinema com Pipoca temático**
Público-alvo prioritário: Operacional.

Exibição de filme ligado à Segurança da Informação em parceria com a área da biblioteca central, com sorteio de livros ao final da exibição. A sessão foi realizada no auditório da empresa, o filme foi exibido em dois horários e contava também com distribuição de pipoca e refrigerante. Toda sessão era precedida de breves palavras do gestor da segurança da informação que falava da importância da política de segurança e do seu cumprimento.

Para essa ação foi contratada uma empresa especializada que detinha os direitos autorais para projeção do filme. O filme escolhido foi Duro de Matar 4.0- Sinopse: Os Estados Unidos sofrem um novo ataque terrorista, desta vez através da informática. Um hacker consegue invadir a infraestrutura computadorizada que controla as comunicações, transporte e energia do país, ameaçando causar um gigantesco blecaute. O autor do ataque planejou todos os passos envolvidos, mas não contava que John McClane (Bruce Willis), um policial da velha guarda, fosse chamado para confrontá-lo.

6. **Cartilha de Segurança na Internet do Cert.br**
Público-alvo prioritário: Tático e operacional.

O Cert.br é o Grupo de respostas a incidentes de segurança para a internet brasileira, mantido pelo Comitê Gestor da Internet no Brasil. Além do tratamento de incidentes, treinamento e conscientização e análise de tendência de ataque (CERT, 2016).

A cartilha é um documento com recomendações e dicas sobre como o usuário de internet deve se comportar para aumentar sua segurança e se proteger de possíveis ameaças. Esta cartilha é disponibilizada sob a licença "*Creative Commons*- Atribuição- Uso não comercial- Vedada a criação de obras derivadas 3.0 Brasil". Esta licença dá a liberdade para compartilhar, ou seja, copiar, distribuir e transmitir a obra entre os empregados da companhia, sendo que, para isso, deve-se creditar a obra da forma especificada pelo autor, não podendo utilizá-la para fins comerciais e não podendo alterar, transformar ou criar novas versões com base na obra original.

A cartilha foi disponibilizada em formato digital (PDF) via intranet e também impressa, em parceria com o Cert.br que forneceu as cartilhas impressas. A capa da cartilha e dos seus fascículos estão demonstrado na figura 4.

Figura 4: Capas das cartilhas se fascículos do Cert.br

7. **Vitrine de ideias inovadoras no Sistema de Inovação para melhorar a Segurança da Informação na empresa**
Público-alvo prioritário: Todos.

A companhia possui um sistema de gestão da inovação que faz a captação, avaliação e tratamento das propostas de inovação corporativa. O sistema permite que qualquer colaborador cadastre ideias inovadoras para atender a alguns objetivos corporativos pré-estabelecidos, como, por exemplo: "redução de custos", "otimização de processos internos", "melhoria da satisfação dos clientes", entre outros.

Em parceria com a área responsável em administrar o sistema de gestão de inovação, foi criado uma nova categoria para captação de ideias, chamada de "vitrine

de ideias", durante a campanha de conscientização, sobre o tema segurança da informação, conforme demonstrado na figura 5.

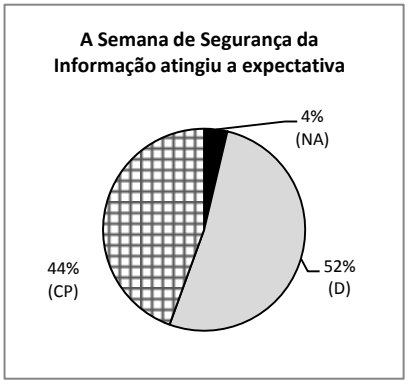
Figura 5: Tela principal do sistema de inovação

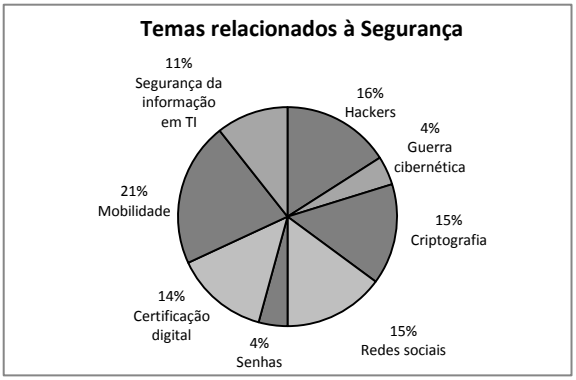
5. Resultados

Após realização das atividades, foi enviada via intranet para os 78 colaboradores participantes das palestras uma pesquisa de satisfação, onde 27 responderam, ou seja, 34% do universo. Como metodologia de medição foi utilizada a escala de Likert, com opções que variam de "Não se aplica", seguida por "Discordo Plenamente", "Discordo", "Concordo" até "Concordo Plenamente". A legenda abaixo serve como referência para os gráficos que utilizaram a referida escala demonstrada abaixo.

- Não se aplica (NA)
- Discordo Plenamente (DP)
- Discordo (D)
- Concordo (C)
- Concordo Plenamente (CP)

Em uma análise geral da campanha, os respondentes avaliaram três itens: a relevância dos temas para a empresa, a expectativa do colaborador quanto ao evento e temas relacionados à Segurança que os colaboradores gostariam de saber mais.

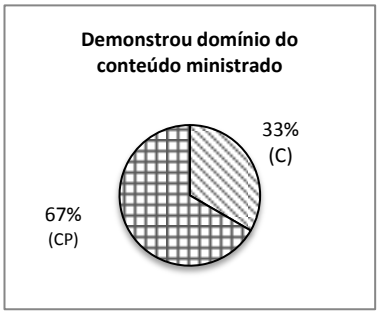


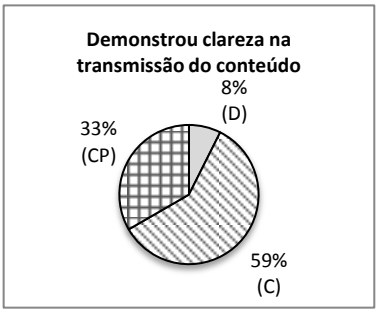


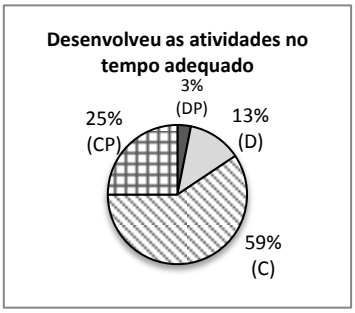
Para avaliar as ações de conscientização utilizadas, os participantes foram questionados sobre que ações chamaram mais sua atenção e colaborou para melhor entendimento e fixação dos temas. Segue abaixo o ranking das ações mais votadas.

Ranking	
Palestras	1º
Vídeo com os empregados	2º
Jogo virtual	3º
Dicas no NE	4º
Cartilha de Segurança do Cert	5º
Cinema com Pipoca	6º
Vitrine de ideias inovadoras	7º

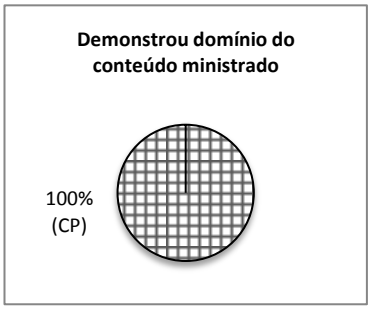
Os palestrantes também foram avaliados. Dentre os itens avaliados estão: domínio do conteúdo, clareza e tempo depreendido. Os gráficos abaixo demonstram as opiniões referentes ao palestrante General Marconi Reis:

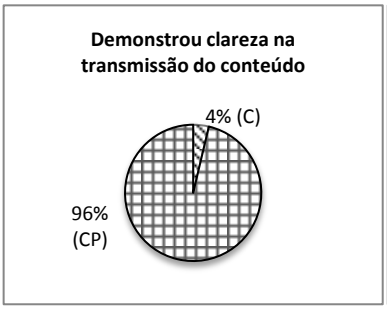


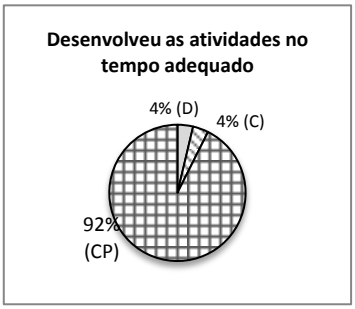




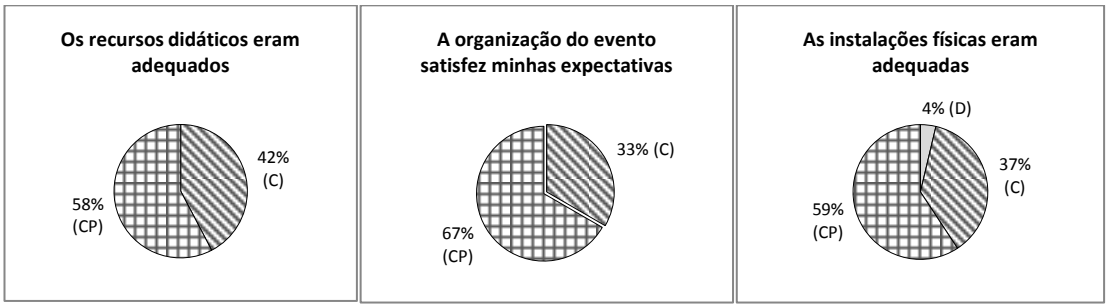
Os gráficos abaixo demonstram as opiniões referentes à palestrante Patrícia Peck:







Também foram avaliadas, as metodologias utilizadas, como, os recursos didáticos adequados, expectativas quanto à satisfação da organização do evento de conscientização e as instalações físicas adequadas.



6. Conclusões

Este artigo apresentou um estudo de caso sobre Campanhas de Conscientização em Segurança da Informação em uma empresa do setor elétrico brasileiro. Uma ação de conscientização tem o objetivo de focar a atenção sobre um determinado assunto e no atual ambiente corporativo, é fundamental que os colaboradores sejam conscientizados sobre seu papel e responsabilidades sobre o assunto tratado. De acordo com a norma ISO 27002, convêm 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.

O sucesso da campanha pôde ser medido, primeiro por ter sido tratado como um projeto que de acordo com as boas práticas PMI descritos no Guia de Gerenciamentos de Projetos – PMBoK –, que é um esforço temporário empreendido para criar um produto, serviço ou resultado exclusivo. E também por ter sido realizada uma pesquisa de satisfação com os participantes, que mediu os seguintes itens: Relevância do tema para a empresa, a expectativa do colaborador quanto ao evento e tópicos de interesse futuro.

Como tema para as próximas campanhas os respondentes indicaram os temas: mobilidade, hackers, redes sociais, criptografia, certificação digital, segurança da informação em TI, senhas e guerra cibernética.

Como lições aprendidas, foi a formalização em projeto, parceria com diversas áreas, como Comunicação, RH, Biblioteca, entre outros, e o rankeamento dos tópicos para priorizar para as próximas campanhas.

O resultado obtido com a campanha de segurança da informação foi satisfatório e demonstrou uma boa aceitação por parte dos colaboradores.

7. Referências

ABNT NBR ISO/IEC 27001. Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos, 2ª Edição, 2013.

ABNT NBR ISO/IEC 27002. Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação, 2ª Edição, 2013.

ALIMAQOUSI, BALIKHINA T., MACKAY M.- An effective method for information Security Awareness Raising Initiatives. International Journal of Computer Science & Information Technology (IJCSIT) Vol. 5, No 2, April 2013.

BASTO, FABRICIO. Política de Segurança da Informação – Como fazer?- Janeiro, 2015- Disponível em: http://analistati.com/politica-de-seguranca-da-informacao-como-fazer/ Acessado em: 11/01/2016.

CERT.br- Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil- Cartilha de Segurança para Internet. Disponível em: http://www.cert.br/sobre/

GROSS, J. B. & ROSSON. Looking for trouble: understanding end-user security management. In *Proceedings of the 2007 symposium on Computer human interaction for the management of information technology*, CHIMIT '07, New York, NY, USA. ACM.

GUELMAN, LUIZ. Módulo News, Agosto, 2006- Disponível em: http://www.modulo.com.br/comunidade/entrevistas/616-conscientizacao-de-usuarios-como-envolver-seu-publico-com-a-seguranca-da-informacao

KRUGER H.A., DREVIN L., STEYN T.. A framework for evaluating ICT security awareness.http://www.computer.org/portal/site/security/menuitem.6f7b2414551cb84651286b108bcd45f3/index. sp?&pName=security_level1_article&TheCat=1001&path=security/2006/v4n5&file=bsi.xml& May,2008

NIST SPECIAL PUBLICATION 800-16. Computer Security- Information Technology Security Training Requirements: A Role-and Performance-Based Model, version 1.0, 1998

NIST SPECIAL PUBLICATION 800-50. Computer Security- Building an Information Technology Security Awareness and Training Program, Version 1.0, 2003.

PCI DATA SECURITY STANDARD. Information Supplement: Best Practices for Implementing a Security Awareness Program, Version 1.0, 2014.

PROJECT MANAGEMENT INSTITUTE. A Guide to the Project Management Body of Knowledge,5ª Edição, 2013.

YIN, ROBERT K.. Estudo de caso: Planejamento e Métodos, 5ª Edição, Porto Alegre, 2015.

SÊMOLA, Marcos. Gestão da Segurança da Informação: uma visão executiva - Rio de Janeiro: Campus, 2004.