Práticas de Disseminação de Conhecimentos em Segurança Cibernética e Lei Geral de Proteção de Dados Pessoais

Conference Paper · March 2023

CITATIONS
0

READS
39

8 authors, including:

Andre Azevedo Pretini
Instituto Nacional de Telecomunicações
1 PUBLICATION **0** CITATIONS
SEE PROFILE

Olívia C. B. Santos
Instituto Nacional de Telecomunicações
1 PUBLICATION **0** CITATIONS
SEE PROFILE

Eduardo Henrique Teixeira
Instituto Nacional de Telecomunicações
11 PUBLICATIONS **13** CITATIONS
SEE PROFILE

André Nascimento
Instituto Nacional de Telecomunicações
1 PUBLICATION **0** CITATIONS
SEE PROFILE

Práticas de Disseminação de Conhecimentos em Segurança Cibernética e Lei Geral de Proteção de Dados Pessoais

André A. Pretini[1], Olívia C. B. Santos[1], Thiago H. O. Campos[1], Eduardo H. Teixeira[1,2], André do Nascimento[1], Patrícia G. da Silva[2], Guilherme P. Aquino[1], Evandro C. Vilas Boas[1]

[1]Centro de Segurança Cibernética do Inatel (CxSC Telecom)
Instituto Nacional de Telecomunicações (Inatel)
Caixa Postal 37540-000 – Santa Rita do Sapucaí – MG – Brasil

[2]Programa de Pós-Graduação em Ensino Profissional e Tecnológico (PPG EPT)
Instituto Federal do Rio de Janeiro (IFRJ)
Caixa Postal 17250-000 – Rio de Janeiro – RJ – Brasil

andre.azevedo@gea.inatel.br, olivia.carvalho@get.inatel.br,

thiago.th@get.inatel.br, eduardot@gea.inatel.br,

patricia.grasel@ifrj.edu.br, guilhermeaquino@inatel.br,

evandro.cesar@inatel.br

Abstract. *This work reports the experience and results obtained by the Inatel Cybersecurity Center (CxSC Telecom Inatel) in developing practices for disseminating knowledge on cybersecurity and LGPD for protecting personal data regarding the institutional and social sphere. First, practical activities are discussed, emphasizing them in the training and qualification process of professionals, undergraduate, and secondary/technical education students. Then, it presents materials derived from the developed practices, including lectures, webinars, scientific articles, educational handouts, white papers, and professional training courses. Finally, it discusses future actions to expand the scope of activities.*

Resumo. *Este trabalho relata a experiência e resultados obtidos pelo Centro de Segurança Cibernética do Inatel (CxSC Telecom Inatel) no desenvolvimento de práticas de disseminação de conhecimento em segurança cibernética e LGPD para proteção de dados pessoais no âmbito institucional e social. Discutem-se as atividades práticas enfatizando-as no processo de formação e capacitação de profissionais, alunos de cursos de graduação e ensino médio/técnico. Por conseguinte, apresentam-se os materiais derivados das práticas desenvolvidas, incluindo palestras, webinars, artigos científicos, apostilas educativas, white papers e cursos de formação e capacitação profissionais. Conclui-se o trabalho discutindo ações futuras para expansão do escopo de atividades.*

1. Introdução

O progresso nos campos das tecnologias da informação e comunicação (TICs) e a evolução contínua de sistemas e redes de telecomunicações contribuem para a aceleração

da transformação digital dentro de instituições. Por conseguinte, expandem-se os domínios do mundo digital oferecendo uma gama maior de aplicações e serviços e contribuindo para a conectividade em massa de dispositivos e pessoas que visam consumi-los [Zhang et al. 2018]. A digitalização abrange processos ou atividades rotineiras, inicialmente executados de forma física, favorecendo o aumento de fluxo de dados por meios digitais para assegurar a continuidade dos procedimentos, por exemplo, o desenvolvimento das linhas de serviços de uma instituição. Todavia, muitos desses dados são considerados pessoais e sensíveis e devem trafegar pelos meios de comunicação, serem tratados e armazenados de forma segura utilizando de aparatos tecnológicos amparados por procedimentos adequados que os protejam de acessos indevidos e não autorizados [Zhou et al. 2019].

Nesse contexto, a segurança cibernética surge como um campo do conhecimento dedicado a prover tais tecnologias e desenvolver processos baseados em boas práticas, além de trabalhar o aspecto humano através da formação e capacitação profissional. Ao explorar a tríade: processos, figura humana e tecnologias, a segurança cibernética permite construir soluções tecnológicas seguras por meio de profissionais capacitados em operá-las para proteger sistemas e redes de telecomunicações, incluindo soluções em tratamento e armazenamento, de ataques digitais com foco em acessar, alterar, destruir ou sequestrar dados e informações para obter vantagens financeiras, como a extorsão de pessoas e empresas [Li et al. 2016]. Ressalta-se que qualquer instituição está exposta aos ataques cibernéticos durante a condução de suas vias de serviços, visto que a conectividade com a Internet é essencial ao mesmo tempo que expõem sua infraestrutura de rede e ativos.

Torna-se crucial que instituições pratiquem o investimento contínuo em soluções tecnológicas conjuntas à formação e capacitação de profissionais para fomentar processos seguros, visando manter suas defesas atualizadas em relação a evolução tecnológica dos ataques cibernéticos [Pasqualetti et al. 2013, Humayed et al. 2017]. Consequentemente, deve-se amparar esse processo em uma política de gestão de riscos, compreendendo todo o ciclo de vida do dado em questão. Falhas no processo de gestão dos dados pode criar possíveis vulnerabilidades, expondo-os ao vazamento por meio de ataques cibernéticos. Além disso, treinamento e conscientização de funcionários é fundamental para a segurança da informação, visto que a figura humana é fator recorrente para exploração de vulnerabilidades através de técnicas de Engenharia Social. Com isso, as instituições são capazes de evitar problemas graves de segurança que possam causar prejuízos diversos, principalmente, danos públicos à imagem perante os serviços que oferecem [Pinheiro 2020].

A definição dos processos e boas práticas em segurança cibernética são norteadas por um conjunto de conceitos, denominados de pilares da segurança cibernética, que definem as soluções tecnológicas para suporte. Inicialmente, esses pilares correspondiam a tríade: confidencialidade, integridade e disponibilidade [Moschovitis 2021]. Posteriormente, o contexto tecnológico atual levou a inclusão de outros dois fatores, a autenticidade e a irretratabilidade. Em suma, a confidencialidade confere o acesso aos dados apenas às pessoas autorizadas. Por outro lado, a integridade visa evitar que os dados sejam indevidamente adulterados durante o processo de tratamento ou armazenamento. A disponibilidade tem o objetivo de prover acesso aos dados a qualquer momento e de qualquer lugar sempre que um usuário com acesso permitido o requisitar. Por conseguinte, a autenticidade visa garantir que uma entidade seja realmente quem diz ser. Enquanto

que o conceito de irretratabilidade ou não repúdio, se aplica a garantir que uma entidade não possa negar sua participação em qualquer evento ou transação relacionada ao acesso, transmissão ou alteração de dados.

A segurança cibernética tem aplicações tanto no âmbito institucional quanto pessoal. Em ambientes institucionais, os dados são cruciais para desenvolvimento dos serviços prestados e devem ser protegidos durante todo o ciclo de vida, com base nos conceitos mencionados anteriormente para prover um ambiente seguro e credibilidade para a instituição perante os usuários. Na esfera pessoal, a segurança cibernética visa garantir princípios fundamentais aos cidadãos para acessos digitais e compartilhamento de informações e dados pessoais, protegendo-os contra o uso não autorizado e indevido de seus dados [Trento 2021]. No Brasil, aprovou-se a Lei Geral de Proteção de Dados (LGPD) em agosto de 2020, estabelecendo regras para o uso e tratamento de dados pessoais [Botelho 2020]. A lei prevê a proteção dos dados relacionados às pessoas físicas e/ou jurídicas ao longo de todo o ciclo de vida das informações, desde a sua aquisição até o descarte. Em casos de violação e exposição dos dados, a lei define diretrizes administrativas que as empresas devem seguir, inclusive a notificação aos donos desses dados. Está prevista também a fiscalização por parte da Autoridade Nacional de Proteção de Dados (ANPD), órgão de estância federal responsável por cumprir a LGPD e aplicar sanções por descumpri-la [de Teffé and Viola 2020].

Referente as discussões anteriores, verifica-se a necessidade de práticas de disseminação de conhecimentos em segurança cibernética e LGPD focadas na formação e capacitação da figura humana para atuação responsável dentro de ambientes tecnológicos e convívio seguro em uma sociedade digital, abrangendo o âmbito institucional e social. Dessa forma, o Centro de Segurança Cibernética do Inatel (CxSC Telecom Inatel) desenvolveu e formatou um conjunto de atividades práticas direcionadas à formação e capacitação de profissionais, alunos de cursos de graduação e ensino médio/técnico. Ademais, tais práticas contribuíram para a elaboração de diversos materiais, incluindo palestras, *webinars*, artigos científicos, apostilas educativas, *white papers* e cursos de formação e capacitação profissionais. Nesse trabalho, relata-se a experiência e os resultados obtidos no desenvolvimento dessas atividades práticas como forma de estimular essa abordagem por outras instituições, sejam empresariais ou de ensino. Ainda no foco da disseminação de conhecimentos, são citados os materiais criados como forma de divulgação e apoio a outras instituições na construção de atividades similares.

O restante do trabalho está estruturado da seguinte forma: Na Seção 2, contextualizam-se os fundamentos da segurança cibernética e ataques comuns como forma de demonstrar que a conscientização é fundamental para trabalhar a figura humana. Posteriormente, conceitos básicos da LGPD são inclusos alinhando-se as atividades desenvolvidas. Na Seção 3, descrevem-se as atividades práticas desenvolvidas agrupando-as em atuação em capacitação profissional, capacitação educacional e disseminação de conteúdo. Considerações e trabalhos futuros encontram-se na Seção 4.

2. Importância da Disseminação de Conhecimentos em Segurança Cibernética e LGPD

A figura humana constitui um fator essencial na construção de um ambiente tecnológico seguro do ponto de vista institucional. Em outras palavras, a conscientização sobre as-

pectos de segurança cibernética por parte de um colaborador, independentemente de seu papel na instituição, é primordial para assegurar a correta execução de procedimentos pautados em prover segurança cibernética. Da mesma forma, operar de forma correta as tecnologias que asseguram os pilares da segurança cibernética, potencializa sua eficácia em proteger os ativos físicos e digitais de uma instituição [Souza et al. 2022]. Agentes maliciosos utilizam-se desse aspecto para invadir e violar a segurança cibernética de dispositivos eletrônicos (pessoais ou institucionais) através da figura humana, cujas abordagens são diversas e denominadas de técnicas de Engenharia Social.

A Engenharia Social explora estratégias de persuasão, intimidação, bajulação e assistência como forma de explorar o viés humano em influenciar ações e/ou obter informações chaves na descoberta de vulnerabilidades em redes de comunicação institucionais ou pessoais [Souza et al. 2022]. Essas estratégias são viabilizadas por meio de mídias socias empregando técnicas conhecidas como *phishing*, *spear phishing*, *vishing*, *smishing*, personificação entre diversas outras. Em termos gerais, *phishing* é uma prática comum que visa conseguir informações de pessoas sem vasto *know-how* em segurança digital ou no uso de tecnologias, para obter senhas bancárias e detalhes confidenciais. A abordagem à vítima ocorre por meio de *e-mail* elaborados para passarem por autênticos e confiáveis. O conteúdo apresentado por *e-mail* visa extorquir a vítima financeiramente ou persuadi-la a realizar uma determinada ação com o objetivo de capturar dados confidenciais ou desencadear a execução ou instalação de códigos maliciosos (*malwares*) [Edraki et al. 2021].

Campanhas de *phishing* para disseminar *malwares* são comuns nos dias atuais, sendo a modalidade *ransomware* amplamente difundida pelos agentes maliciosos com foco em ambientes institucionais [Vilas Boas and Aquino 2022]. Variações do *phishing* também são comuns e conhecidas como *spear phishing*, *vishing* e *smishing*. Em suma, o *spear phishing* relaciona-se a direcionar a campanha as práticas do *phishing* para um indíviduo específico. O *vishing* e *smishing* referem-se ao uso de voz e mensagens de texto como meios de obter informações ou influenciar ações através de dispositivos móveis. Por fim, os agentes maliciosos podem utilizar dos meios de comunicação para personificar pessoas próximas e conhecidas da vítima para obter vantagem financeira ou informações confidenciais, por exemplo, utilizando aplicativos de conversa.

Verifica-se que os ataques cibernéticos mais comuns se apoiam na falta de conhecimento de pessoas e vulnerabilidades dos sistemas e redes de telecomunicação para a execução com sucesso. Logo, a LGPD entrou em vigor para regulamentar e garantir o direito a proteção e privacidade de dados pessoais utilizados por empresas no desenvolvimento de seus negócios, seja no meio digital ou físico [Pinheiro 2020]. Em suas diretrizes, a lei discorre sobre os direitos do titular dos dados, a finalidade de tratamento desses dados, define os envolvidos no processo de tratamento e fiscalização da operação dos dados pessoais em uma organização e sanções em caso de descumprimento por meio de multas. A legislação vigente deve ser cumprida por empresas que fazem a utilização dos dados pessoais. Por isso é necessário instruir a população sobre a importância dos dados pessoais e sobre os direitos fundamentais como a liberdade e a privacidade, sendo o descumprimento dessas regras passível de sanções e multas [de Teffé and Viola 2020].

A LGPD assegura ao titular dos dados todos os direitos previstos em lei enquanto sob a custodia de alguém. Conforme declara o artigo 1º da Lei Geral de Proteção de

Dados, seu intuito é assegurar os direitos fundamentais de liberdade e privacidade. A proteção de direitos se baseia em procedimentos de segurança que devem ser obedecidos durante o ciclo dos dados em posse de alguém, impedindo atos ilegais ou antiéticos [Pinheiro 2020]. A transparência da informação garante ao titular um acesso livre ao que está sendo realizado com seus dados por terceiros, preservando privacidade, liberdade de expressão, comunicação, opinião, intimidade, honra, imagem, direitos humanos e dignidade [Yu et al. 2017]. No âmbito da legislação, classificam-se os dados em três tipos: dados pessoais, sensíveis e anonimizados [de Aragão and Schiocchet 2020]. Os dados pessoais referem-se àqueles de uma pessoa física identificada ou identificável. Os dados sensíveis remetem-se às informações de cunho individual como origem étnica, opinião política, orientação religiosa, orientação sexual, dado genético ou biométrico. Já os dados anonimizados compreendem aqueles em que o titular não pode ser identificado. A LGPD visa a proteção dentro da legislação a qualquer pessoa física identificada ou não identificável.

3. Práticas de Disseminação de Conhecimentos em Segurança Cibernética e LGPD

A prática de disseminação de conhecimentos na área de segurança cibernética é um instrumento pelo qual pode-se prover a formação e capacitação de pessoas em diferentes contextos, sendo aqueles relacionados ao institucional e social explorados no escopo das atividades propostas pelo CxSC Telecom. Para as instituições, atividades em formação e capacitação profissional com foco em assuntos de segurança cibernética contribuem para a conscientização sobre o papel da figura humana nos processos definidos para resguardar os ativos físicos e digitais. Em sociedade, desenvolvem-se as práticas por meio de facilitadores para transmissão de conhecimentos em segurança cibernética, construindo o entendimento da pessoa em um contexto digital de ameaças. Com isso, essa pessoa torna-se ciente quanto as medidas básicas para evitar essas ameaças, tendo como base seus direitos enquanto titular de seus dados, com base no que é disposto na LGPD e através do conhecimento sobre as formas seguras de se compartilhar e acessar informações. Portanto, apresentam-se o conjunto de atividades desenvolvidas pelo CxSC Telecom com foco em capacitação profissional, capacitação de estudantes e disseminação de conteúdos.

3.1. Práticas para capacitação profissional

As práticas para a formação e capacitação profissional compreendem a elaboração e oferta de cursos relacionados à segurança cibernética em redes e sistemas de telecomunicações, conforme visto na Figura 1. Profissionais ligados ao CxSC Telecom e com formação prévia na área contribuíram para a entrega de cursos em Segurança Cibernética em Redes de Telecomunicações e Segurança Cibernética para Redes Móveis de Quinta Geração (5G). Essas atividades foram ofertadas para profissionais ligados a empresas provedoras de redes de telecomunicações, utilizando a infraestrutura física de instituições parceiras para que a oferta fosse em modelo presencial. O curso também foi replicado aos alunos de graduação dos cursos de engenharia do Inatel e os materiais utilizados foram compilados em cursos online oferecidos de forma contínua pela plataforma Inatel *Online*, os quais podem ser adquiridos por qualquer profissional que deseje ter acesso aos conteúdos desse material.

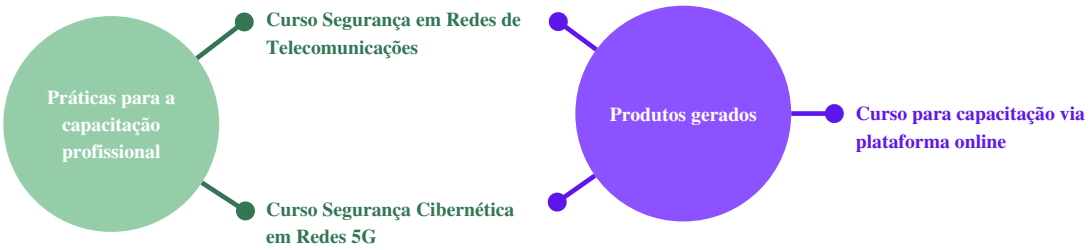

Figura 1. Práticas de capacitação profissional e produtos gerados.

Elaboraram-se os cursos com foco nos aparatos tecnológicos necessários para prover os recursos em segurança cibernética no projeto de redes e sistemas de telecomunicações. Os pilares da segurança cibernética foram explorados de forma a expandir o conhecimento do profissional quanto as soluções tecnológicas disponíveis para projeto de infraestrutura de redes seguras. Discutiram-se os protocolos de comunicação segura, contextualizando-os no dia-a-dia do ouvinte para facilitar a assimilação e entendimento do conteúdo. Por fim, demonstrações práticas foram conduzidas com o intuito de ressaltar como a presença dos aparatos tecnológicos contribuem para prover camadas de segurança em uma infraestrutura de rede, mas são factíveis de falha quando a figura humana não está apta a operá-las de forma correta. Como resultado dessa atividade, o CxSC capacitou cerca de 200 profissionais em atuação ou em formação no ano de 2022.

3.2. Práticas para capacitação de estudantes

No contexto da formação de estudantes, as atividades práticas compreendem a atuação com alunos de graduação e escolas da rede pública e privada de ensino a nível médio e técnico da região do Sul de Minas e São Paulo, por meio de projetos de extensão educacional em segurança cibernética, redes de telecomunicações e LGPD. Tais projetos referem-se a competição *Telecom Challenge* – Desafio *Hacker* e aos programa de Capítulos de segurança cibernética (CxSC - *Chapter*), que promove eventos, palestras, *workshops* e minicursos, como indicado na Figura 2.

Figura 2. Práticas de capacitação de estudantes e produtos gerados.

O CxSC *Chapter* é organizado em formato de grupos ou grêmios estudantis em escolas regionais parcerias [Inatel 2023]. A estrutura básica compreende grupos de alunos com 10 ou 15 integrantes orientados localmente por um tutor ou professor designado pela escola parceira que acompanha as atividades propostas e desenvolvidas pelos agentes do CxSC Telecom em formato *online* e presencial. Durante o ano de 2022, três unidades foram consolidadas na região do Sul de Minas, compreendendo escolas das cidades de

Brasópolis, Campanha e Santa Rita do Sapucaí, sendo uma quarta unidade em processo de formação na cidade de Pouso Alegre.

Nesse projeto, os membros de cada capítulo recebem materiais que abordam conceitos de segurança cibernética relacionados ao uso de aplicativos móveis, serviços *web*, redes sociais, e compartilhamento de informações pessoais na Internet, com foco nas diretrizes de proteção de dados norteados pela LGPD. Inicialmente, é instigado ao professor tutor desenvolver o estudo e discussões sobre o tema e, posteriormente, essa discussão é revisitada pelos agentes do CxSC Telecom para expandir o entendimento, esclarecer dúvidas e dar exemplos práticos e cotidianos de forma a conduzir a absorção do conteúdo. Cada ciclo de estudo é concluído com uma atividade prática que visa apresentar tecnologias relacionadas aos assuntos discutidos para fortalecer a formação tecnológica e incentivar os membros do CxSC *Chapter* a aderirem a área como opção de carreira.

Além disso, o CxSC Telecom também desenvolve atividades no formato de desafios referentes ao escopo do projeto *Telecom Challenge* - Desafio *Hacker* que visa difundir conhecimentos na área de segurança cibernética, redes de computadores, telecomunicações e LGPD. Esse projeto é estruturado em três etapas definidas como preparação, treinamento e torneio. A preparação corresponde as atividades de estudo e compreensão dos conceitos relacionados as áreas supracitadas, onde os participantes recebem material didático em formato de apostilas educativas. O conteúdo dessas apostilas é explorado por meio de discussões e exemplos apresentados aos participantes em formato de aulas *online* síncronas e também vídeos curtos pela plataforma *YouTube* para acesso sob demanda. Por conseguinte, tem-se a etapa de treinamento que integra competições para introdução do participante a dinâmica do torneio e familiaridade com a plataforma de jogo, CTF.io. O uso da plataforma permite aos participantes realizarem um processo de revisão dos conteúdos estudados ao longo dos módulos, bem como um primeiro contato com as TICs que suportam seu funcionamento e navegabilidade. Por fim, ocorre o torneio dividido em duas categorias, individual e em grupo, cada qual com fases eliminatórias e final.

A plataforma CTF.io foi adotada por prover funcionalidades tecnológicas que facilitam a gamificação do ensino em um ambiente lúdico e ao mesmo tempo *online* para expandir o alcance do projeto, conectando participantes dos estados de Minas Gerais, São Paulo e Rio de Janeiro por meio das TICs. A plataforma é baseada em competições no estilo *Capture the Flag* [McDaniel et al. 2016], apresentando problemas ao participante acerca do assunto previamente estudado, neste caso, segurança cibernética, redes de computadores, telecomunicações e as diretrizes da LGPD [Botelho 2020]. Para obter a pontuação e o melhor posicionamento no *ranking*, deve-se decifrar os desafios e fornecer a resposta de forma correta no menor tempo possível. Emprega-se a gamificação aplicada ao ensino tradicional como forma de desenvolvimento de metodologias inovadoras, buscando estimular a participação de alunos em diversas atividades para desenvolver habilidades e competências na área correlata. A plataforma também permite ofertar dicas para a solução dos desafios ao custo de uma parcela da pontuação acumulada. Com isso, além de conhecimentos técnicos, outras competências são desenvolvidas, como a administração de recursos e riscos, inerentes aos projetos de engenharia, bem como outras áreas em que esses alunos possam atuar futuramente.

O projeto reuniu centenas de alunos de escolas dos estados de Minas Gerais, São

Paulo e Rio de Janeiro. Na primeira edição, inscreveram-se cerca de 130 alunos, dos quais 92 se inscreveram na categoria individual e 60 deles na categoria em grupo. Na segunda edição, 250 alunos se inscreveram, sendo 118 participantes na categoria individual e 173 na categoria em grupo. Na terceira edição foram 219 estudantes inscritos, sendo 108 participantes na categoria individual e 141 na categoria em grupo. Vale ressaltar que existem alunos que participam das duas categorias concomitantemente. A divulgação das inscrições para o torneio ocorre através das redes sociais dos setores do Inatel e também da divulgação orgânica, realizada por membros que participaram das primeiras edições. Como a participação é aberta ao público, o *Telecom Challenge* - Desafio *Hacker* também é utilizado para convidar outras instituições a participarem dos Capítulos CxSC Telecom. Com isso, as atividades de disseminação de conhecimentos em segurança cibernética sempre estão evoluindo e vem crescendo em intensidade ao longo do projeto.

3.3. Práticas de disseminação de conteúdos

As práticas de disseminação de conteúdos em segurança cibernética incluem geração e publicação de artigos científicos e *white papers*, promoção de *webinars*, palestras e workshops, assim como publicação de conteúdos em perfis educativos em redes sociais. A participação em congressos e simpósios nacionais permite ao CxSC Telecom fomentar discussões inerentes ao mercado de segurança cibernética e conectá-lo com o ambiente acadêmico de forma a criar vias de diálogo entre as partes. Dessa forma, o CxSC Telecom participou do Simpósio Brasileiro de Telecomunicações 2022 promovendo um painel de discussão com o tema "Os problemas e Soluções de Segurança Cibernética nas Diferentes Infraestruturas Críticas". Por outro lado, contribuiu para o conhecimento científico com publicações relacionadas a segurança cibernética no âmbito tecnológico [Tacca et al. 2022, Casagrande et al. 2022].

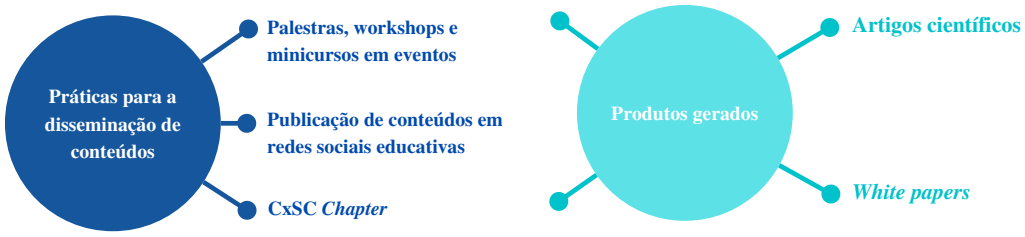

Figura 3. Práticas de disseminação de conteúdos e produtos gerados.

Palestras trouxeram temas importantes para discussão em uma esfera institucional e social. Dessa forma, contribui-se para eventos como a Semana de Telecomunicações do Inatel e Mind The Sec. Em contrapartida e visando uma abrangência ampla, *webinars* foram difundidos por meio da plataforma *YouTube* e disponíveis sob demanda, abrangendo assuntos técnicos e humanos. Destaca-se o *webinars* intitulado "Engenharia Social: A figura humana como falha de segurança" que trouxe uma reflexão sobre como o elemento humano é facilmente coibido pelas práticas da Engenharia Social e torna-se um aspecto factível a criar vulnerabilidades em instituições ou ser explorado em cunho social. As palestras e *webinars* fomentaram a escrita de *white papers* que complementam os eventos e provêm uma visão ampla dos assuntos pautados, sendo disponibilizados através do *website* do CxSC Telecom [Vilas Boas et al. 2022, Souza et al. 2022].

4. Conclusão e Trabalhos Futuros

Este trabalho relatou a experiência e os resultados obtidos pelo CxSC Telecom no desenvolvimento de atividades práticas de disseminação de conhecimento em segurança cibernética e LGPD no contexto institucional e social, com foco na comunidade regional. Por conseguinte, as atividades práticas foram apresentadas e enfatizadas no processo de formação e capacitação de profissionais, alunos de cursos de graduação e ensino médio/técnico. Assim como, incluíram-se práticas de divulgação ampla para a sociedade em geral por meio de publicações acadêmicas, promoção de palestras e participação em eventos como feiras, congressos e simpósios, além de *webinars* transmitidos de forma *online* e disponíveis por meio da plataforma multimídia.

Em suma, desenvolveram-se materiais multimídias, apostilas educativas, artigos científicos, *white papers* e competições para gamificação do ensino. Os materiais multimídias apoiaram o processo de capacitação de profissionais e a disseminação de conhecimento para a sociedade geral ao serem disponibilizadas em plataformas *online*. As discuções provenientes desses materiais instigaram discussões e a escrita de *white papers* específicos. Apostilas educativas e a plataforma de competição por meio da gamificação serviram como apoio para levar conhecimento aos alunos de cursos de graduação e ensino médio/técnico de escolas públicas e particulares, conscientizando-os a respeito do assunto e estimulando o interesse pela área. Por fim, esses materiais foram alicerces para a criação de grupos estudantis, denominados de Capítulos CxSC, perpetuando a transferência de aprendizado e formação contínua desses alunos.

Trabalhos futuros incluem a elaboração de materiais para o ensino fundamental, adequando-o para a capacitação de crianças e adolescentes visto que são considerados nativos digitais e vulneráveis ao trabalho da Engenharia Social. Dessa forma, almeja-se ações de conscientização sobre segurança cibernética quanto ao uso de redes sociais, salas e grupos de conversas e amizades virtuais, para que essa cultura seja construída de forma precoce preparando o indivíduo para um convívio social seguro no mundo digital. Ademais, atividades de expansão dos Capítulos CxSC Telecom e organização de novos eventos estão inclusos na pauta desse trabalho. Em âmbito institucional, planeja-se iniciativas relacionadas a execução de novas atividades de formação e capacitação, expandindo as ações prestadas à terceiros e enriquecendo o portfólio de conhecimento dos membros que atuam junto ao CxSC Telecom.

Referências

Botelho, M. C. (2020). A lgpd e a proteção ao tratamento de dados pessoais de crianças e adolescentes. *Revista Direitos Sociais e Políticas Públicas–Unifafibe*, Vol. 8(2):18.

Casagrande, L. V. I. C., Vilas Boas, E. C., and Aquino, G. P. (2022). Systems, software, and applications updating for avoiding cyber attacks: A pentest demonstration. In *XL Simpósio Brasileiro de Telecomunicações e Processamento de Sinais (SBrT2022)*.

de Aragão, S. M. and Schiocchet, T. (2020). Lei geral de proteção de dados: desafio do sistema único de saúde. *Revista Eletrônica de Comunicação, Informação e Inovação em Saúde*, 14(3).

de Teffé, C. S. and Viola, M. (2020). Tratamento de dados pessoais na lgpd: estudo sobre as bases legais. *Civilistica*, Vol. 9(1):1–38.

Edraki, M., Karim, N., Rahnavard, N., Mian, A., and Shah, M. (2021). Odyssey: Creation, analysis and detection of trojan models. *IEEE Transactions on Information Forensics and Security*, 16:4521–4533.

Humayed, A., Lin, J., Li, F., and Luo, B. (2017). Cyber-physical systems security—a survey. *IEEE Internet of Things Journal*, Vol. 4(6):1802–1831.

Inatel (2023). Capítulos cxsc telecom inatel. `https://inatel.br/cxsc/capitulos`.

Li, Y., Dai, W., Ming, Z., and Qiu, M. (2016). Privacy protection for preventing data over-collection in smart city. *IEEE Transactions on Computers*, Vol. 65(5):1339–1350.

McDaniel, L., Talvi, E., and Hay, B. (2016). Capture the flag as cyber security introduction. In *2016 49th Hawaii International Conference on System Sciences (HICSS)*, pages 5479–5486.

Moschovitis, C. (2021). *A Cybersecurity Primer*, volume Vol., pages 181–204.

Pasqualetti, F., Dörfler, F., and Bullo, F. (2013). Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic Control*, Vol. 58(11):2715–2729.

Pinheiro, P. P. (2020). *Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018-LGPD*. Saraiva Educação SA.

Souza, J., Rennó, V., Vilas Boas, E., and Aquino, G. (2022). Engenharia social: A figura humana como falha de segurança. Technical report.

Tacca, A. S., Vilas Boas, E. C., and Aquino, G. P. (2022). Aspectos de segurança cibernética em redes móveis 5g. In *XL Simpósio Brasileiro de Telecomunicações e Processamento de Sinais (SBrT2022)*.

Trento, M. (2021). A inteligência artificial aplicada nos serviços públicos e os principais desafios impostos pela lgpd: The artificial intelligence applied in public services and the main challenges imposed by lgpd. *International Journal of Digital Law*, Vol. 2(1):17–18.

Vilas Boas, E. and Aquino, G. (2022). Ransomware: Prevenção e resposta a incidentes. Technical report.

Vilas Boas, E., Rennó, V., and Aquino, G. (2022). Ransomware: Incident prevention and response. Technical report.

Yu, J., Zhang, B., Kuang, Z., Lin, D., and Fan, J. (2017). iprivacy: Image privacy protection by identifying sensitive objects via deep multi-task learning. *IEEE Transactions on Information Forensics and Security*, Vol. 12(5):1005–1016.

Zhang, J., Chen, B., Zhao, Y., Cheng, X., and Hu, F. (2018). Data security and privacy-preserving in edge computing paradigm: Survey and open issues. *IEEE Access*, Vol. 6:18209–18237.

Zhou, W., Jia, Y., Peng, A., Zhang, Y., and Liu, P. (2019). The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *IEEE Internet of Things Journal*, Vol. 6(2):1606–1616.