Ganesh: um grupo de extensão para ensino de Segurança da Informação do ICMC/USP

Felipe Mendes Salles
ICMC/USP, São Carlos
felipesalles@usp.br

Emelly Marinho
ICMC/USP, São Carlos
emelly.marinho@usp.br

Gabriel Cruz
ICMC/USP, São Carlos
gabriel.melo.cruz@usp.br

Renan Parpinelli Scarpin
ICMC/USP, São Carlos
renanscarpin@usp.br

Kalinka Branco
ICMC/USP, São Carlos
kalinka@icmc.usp.br

ABSTRACT

This article describes the methodology of Ganesh, an extracurricular group at the University of São Paulo (USP) São Carlos, dedicated to promoting knowledge about Information Security among undergraduate students and the technology community. Ganesh began in 2010 as part of a university outreach project that, over the past few years, has developed teaching materials, specialized courses, and workshops, in addition to creating educational projects for public and private schools. Ganesh connects with the public through various outreach initiatives, including their YouTube channel, an annual selection process (PING), and participation in Capture the Flag (CTF) competitions. Using a methodology that combines hands-on learning, challenge solving, and weekly meetings has positioned them among the top teams in Brazil and among the country's top university teams in the best Information Security competitions.

KEYWORDS

Extensão Universitária, Segurança da Informação, Sistemas Web, Educação

1 INTRODUÇÃO

Alcançar uma educação de qualidade[1] é um dos 17 objetivos da ONU para o desenvolvimento sustentável até 2030. Dentre os objetivos específicos, busca-se "aumentar substancialmente o número de jovens e adultos que tenham habilidades relevantes, inclusive competências técnicas e profissionais, para emprego, trabalho decente e empreendedorismo". Desde então, diferentes iniciativas têm sido propostas no mundo para melhorar a educação e oferecer meios de desenvolvimento para jovens e adultos. Por exemplo, o projeto "Codifique" oferecido pelo Programa de Educação Tutorial (PET) Computação [2] realiza um curso para ensinar lógica de programação para estudantes do ensino médio, utilizando a linguagem *Python*.

A dependência da sociedade em sistemas tecnológicos, *Web* e ferramentas multimídia vem aumentando a cada ano, afetando diversas tarefas do cotidiano como educação, saúde e comércio [10, 11]. Uma consequência importante do uso dessas ferramentas digitais é a necessidade de garantir a segurança e a privacidade dos usuários desses sistemas. Sendo assim, um aspecto fundamental amparado pela *Lei Geral de Proteção de Dados* (LGPD) [1].

Mesmo com a aplicação de *frameworks* de segurança, regulamentações e legislações como a LGPD, a confiabilidade dos sistemas é recorrentemente desafiada. Incidentes relacionados a vazamento de dados são noticiados constantemente, como os casos envolvendo Google, Apple e Meta [2], ou ainda, o caso do Banco Neon [5]. Esses episódios reforçam a urgência da sociedade em implementar soluções mais robustas de proteção, além de fomentar uma conscientização mais ampla da sociedade sobre essa realidade.

Com o aumento da demanda por profissionais qualificados para garantir a segurança de sistemas empresariais e governamentais, há pouco otimismo de que a oferta será capaz de suprir tal demanda, pois estima-se uma escassez de aproximadamente 140 mil profissionais de segurança cibernética até 2025 [13]. Por isso, projetos educacionais, que integrem alunos e alunas, surgem como iniciativas fundamentais para disseminar conhecimento na busca pela formação de profissionais qualificados na área.

Contudo, a área de Segurança da Informação pode ser abstrata, tornando, assim, a compreensão e o desenvolvimento de habilidades práticas um desafio considerável para novos estudantes [12]. Nesse contexto, as competições do tipo *Capture The Flag* (CTF) surgem como uma estratégia pedagógica eficaz para o ensino prático de Segurança da Informação [6] ao desafiar os participantes a aplicar suas habilidades em cenários que simulam sistemas reais e vulneráveis, oferecendo uma experiência de aprendizado ativa e prática. Essa abordagem gamificada, além de estimular o engajamento, favorece o desenvolvimento de competências, como pensamento crítico, resolução de problemas, trabalho em equipe e tomada de decisão.

Com esses princípios em mente, alunos do ICMC-USP fundaram em 2010 o Ganesh: grupo de extensão em segurança da informação sediado no Instituto de Ciências Matemáticas e de Computação (ICMC) da USP em São Carlos, que tem como propósito incentivar o aprimoramento dos alunos e alunas em técnicas de segurança digital. Uma das principais funções do grupo é a participação em competições de CTF, onde se destacaram por terem conquistado o 14º lugar global e 1º lugar nacional no *SwampCTF* 2025[3], assim como o 3º lugar global e 1º lugar nacional no *DawgCTF* 2025[4].

Este artigo está dividido como segue: a Seção 2 descreve a origem e a história do projeto de extensão Ganesh, a Seção 3 descreve a estrutura do curso, a Seção 4 discorre sobre os cursos ministrados,

[1] https://brasil.un.org/pt-br/sdgs/4
[2] https://pet.icmc.usp.br/

[3] https://2025.swampctf.com/scoreboard
[4] https://ctftime.org/event/2651

In: IV WebMedia for Everyone (W4E 2025). Anais Estendidos do XXXI Simpósio Brasileiro de Sistemas Multimídia e Web (W4E'2025). Rio de Janeiro/RJ, Brasil. Porto Alegre: Brazilian Computer Society, 2025.

ISSN 2596-1683

a Seção 5 descreve os relatos de alunos e participantes do curso, a Seção 6 descreve os aspectos éticos do projeto e a Seção 7, por fim, discorre sobre as considerações finais.

2 GANESH: HISTÓRIA

Em 2010, alunos ingressantes do curso de Engenharia de Computação (Escola de Engenharia de São Carlos - EESC / Instituto de Ciências Matemáticas e de Computação - ICMC) criaram um grupo de estudos voltado para a área de Administração de Redes e Segurança. Esse grupo foi idealizado inicialmente pelos estudantes Lucas A. M. Magalhães e Luis H. G.Patire. Na fase de concepção, o grupo se inspirou em Ganesha, uma divindade da tradição hindu e védica reconhecida como o deus do intelecto, da sabedoria e da fortuna, dando origem ao nome Ganesh. Desde o princípio, um dos objetivos era criar um espaço para o desenvolvimento de projetos e a realização de eventos que permitissem aplicar, na prática, os conceitos aprendidos. Para consolidar a iniciativa, os alunos buscaram o apoio de docentes que assumiram o papel de tutores, auxiliando no desenvolvimento das atividades do grupo.

A associação à divindade hindu se tornou ainda mais relevante, já que Ganesha é representado na forma de um elefante capaz de colocar e remover obstáculos. Essa metáfora pode ser associada ao propósito do grupo, que buscava compreender as técnicas de segurança para atuar tanto na criação de barreiras contra ataques e vulnerabilidades quanto na proposição de soluções que viabilizassem a segurança de sistemas computacionais. Assim, em 2010, foi oficialmente fundado o grupo Ganesh, que iniciou suas atividades com a missão de unir o estudo coletivo, inclusivo e voltado a desafios práticos para formar estudantes mais qualificados na área de Segurança da Informação. Na Figura 1, é possível visualizar o logo do grupo de extensão.

Figura 1: Logo do grupo de extensão Ganesh - ICMC/USP.

3 CURSOS MINISTRADOS

3.1 PING

O PING (**P**rocesso de **ING**resso) (Figura 2) é a porta de entrada para pessoas interessadas em aprender sobre Segurança da Informação no grupo Ganesh, funcionando como um processo de ingresso com aulas introdutórias ao longo do primeiro semestre. As aulas acontecem duas vezes por semana, com o mesmo conteúdo sendo repetido para atender estudantes tanto externos quanto internos à comunidade USP, que possuem afinidade básica com a área e com diferentes disponibilidades de horário. Na Tabela 1, é possível visualizar o cronograma de atividades da edição de 2025.

Com o objetivo de proporcionar uma base ampla na área de Segurança da Informação, o grupo explora um tema novo a cada semana, abrangendo tópicos essenciais, como: sistemas Linux, Criptografia, Segurança em Redes de Computadores, Segurança Web, Engenharia Reversa, *Pwning*, além de outros temas. Essa metodologia, alinhada à resolução de desafios práticos no formato de CTFs que incentivam a aplicação dos conceitos teóricos e engajam os alunos a desenvolver um entendimento sólido sobre como falhas de segurança ocorrem e como preveni-las em cenários reais.

Tabela 1: Distribuição dos temas por semana no PING 2025.

Semana	Tema	Nº de Aulas
1	Linux	2
2–3	Criptografia	4
4–5	Redes de Computadores	4
6–7	Segurança *Web*	4
8–9	Engenharia Reversa	4
10	*Pwning*	2
11	*OSINT*, *Forense* e Resposta a Incidentes	2

O PING é realizado todos os anos desde 2019, totalizando 7 edições. Em 2025, o projeto passou a realizar transmissões ao vivo pela Internet, nas quais instrutores interagem em tempo real com os comentários dos espectadores, ampliando o alcance do projeto para além da comunidade da USP e assim totalizando 116 participantes. Ao final do PING, aqueles que desejam seguir no Ganesh podem se tornar membros efetivos do grupo. Assim, o PING não é um processo de seleção no qual somente alunos com os melhores resultados podem participar, mas sim de inscrição. Ou seja, qualquer aluno que demonstre interesse e empenho, mesmo sendo da comunidade externa, independentemente de formações anteriores ou grau de dificuldade pessoal, pode fazer parte do grupo. Dessa forma, o PING garante que o Ganesh seja um espaço de formação prática, mas também comunitária e ética, que conecta os estudantes ao universo da Segurança da Informação.

Figura 2: Primeiro dia de aulas do PING 2025 ministrado por membros do Ganesh.

3.2 Semana de Segurança

O projeto de extensão do Ganesh mobiliza alunos de graduação e pós-graduação para organizar a Semana de Segurança, uma iniciativa que oferece à comunidade da USP de São Carlos uma programação intensa de atividades educativas em Segurança da Informação.

O evento promove educação de qualidade com diversos minicursos, palestras e desafios oferecidos pelos membros do grupo. Na edição de 2024, foram ministrados minicursos, como: *Game Hacking*, "HTTPS e TLS: A Proteção da Web", "Uma Visão Geral da Computação *Forense*", *"Lock picking 101"*, "Desenvolvendo Sites Seguros", "Engenharia social: seja a primeira linha de defesa" e "Segurança na era da Internet das Coisas", totalizando aproximadamente 16 horas de minicursos ao longo da semana. Dessa forma, promovendo o ensino de temas importantes e propondo debates relevantes. Ao total, foram atingidas cerca de 60 pessoas.

O público alvo dos cursos ministrados, incluindo a Semana de Segurança, já possui um conhecimento introdutório de computação. Entretanto, ao realizar a transmissão ao vivo dos eventos, possibilitamos que públicos de diferentes níveis de escolaridade possam consumir o conteúdo igualmente.

3.3 Minicursos

Outra iniciativa relevante do Ganesh é a disseminação de conhecimento na área de Segurança da Informação ao oferecer minicursos gratuitos abertos à comunidade. Em 2024, foi promovido o minicurso "Como se sentir mais seguro na internet e não cair em golpes digitais?" com duas sessões presenciais no campus da USP em São Carlos (Figura 3).

Esse minicurso foi organizado por dez membros do Ganesh, sob a coordenação pedagógica de uma docente e com participação direta do coordenador geral do grupo. O objetivo foi promover conscientização e fornecer habilidades práticas para que cidadãos enfrentem os riscos do ambiente digital com mais segurança. A linguagem simples permitiu que o minicurso fosse acessível à comunidade externa à universidade e sem muito conhecimento de computação, com cerca de 20 participantes durante o minicurso.

A realização desses minicursos evidenciam o papel do Ganesh como um projeto consolidado de extensão universitária, visto que possibilita a participação do público geral externo em temas de relevância social, como a criação de senhas seguras, o reconhecimento de *links* maliciosos, noções básicas de Criptografia e informações sobre os direitos do cidadão com o surgimento da *Lei Geral de Proteção de Dados* (LGPD).

4 METODOLOGIA DE ENSINO

O Ganesh disponibiliza diferentes tipos de conteúdos em plataformas de acesso gratuito visando disseminar o conhecimento para todos os interessados na área de Segurança da Informação.

4.1 Aulas Didáticas

A elaboração de aulas didáticas sobre Segurança da Informação por estudantes em um projeto de extensão universitária oferece benefícios significativos tanto para alunos que ministram os cursos quanto para os que participam. Para os instrutores, a preparação do conteúdo requer uma pesquisa aprofundada do tema, uma dedicação à elaboração dos materiais e uma organização didática para que

Figura 3: Oferecimento do minicurso "Como se sentir mais seguro na internet e não cair em golpes digitais?" ministrado por membros do Ganesh.

conceitos complexos sejam ensinados para diferentes níveis de conhecimento. Esse processo contribui significativamente para o desenvolvimento de habilidades de comunicação, permitindo que os membros do Ganesh transformem conhecimento em material gratuito e didático.

Na Figura 4, é apresentado um exemplo prático de aula oferecido pelo Ganesh, para pessoas externas à comunidade com qual qualquer nível de conhecimento chamado de "Segurança Essencial: como estar seguro na internet?". A imagem ilustra o processo de conexão a uma *Virtual Private Network* (VPN), destacando três etapas principais: (1) o processo de autenticação e troca de chaves entre o cliente e o servidor de VPN, garantindo que apenas usuários autorizados possam estabelecer a conexão; (2) a criação de um túnel criptografado, no qual toda a comunicação do cliente é protegida; e (3) a troca de mensagens entre o cliente e o servidor final por meio desse túnel, permitindo que dados sensíveis sejam transmitidos com confidencialidade.

Esse tipo de representação visual é aplicado aos materiais, pois as experiências ao longo dos anos mostraram que os participantes compreendem conceitos abstratos de criptografia e redes de maneira mais concreta.

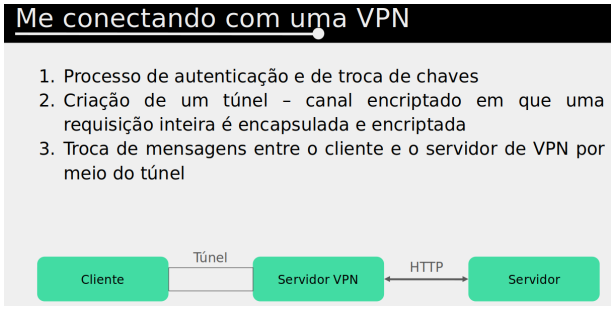


Figura 4: Exemplo de material didático exemplificando a conexão de um cliente com um serviço de VPN desenvolvido por membros do Ganesh para o curso "Segurança Essencial: como estar seguro na internet?".

4.2 Ganesh GitBook

O *Ganesh GitBook* [5] é um site que conta com tutoriais de ensino teórico das bases de Segurança da Informação (Figura 5). Observando o material didático ilustrado na Figura 6, é possível observar a demonstração da utilização do comando "`dig`", presente em sistemas Linux, para a resolução manual de nomes de domínio (*Domain Name System* - DNS). Esse comando permite realizar consultas a servidores de nomes e obter os endereços IP associados a determinado domínio. Assim, os estudantes podem ter seu primeiro contato com conteúdos fundamentais, como, por exemplo, essa compreensão mais concreta do processo de tradução de nomes em endereços de rede.

Figura 5: Ferramenta GitBook Ganesh para divulgação de conteúdos didáticos sobre diferentes tópicos que formam a base para os estudos em Segurança da Informação.

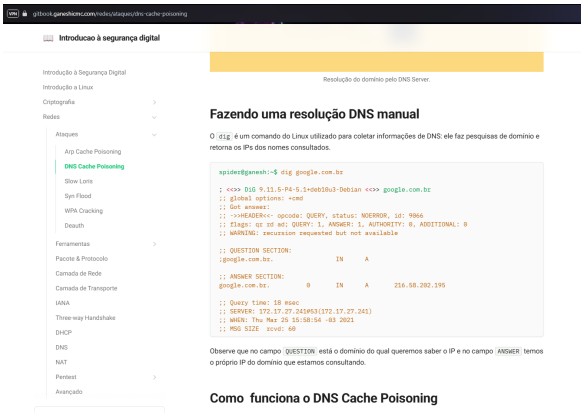


Figura 6: Exemplo de conteúdo didático sobre o uso do comando Linux "dig" utilizado para coletar informações de DNS.

O Ganesh também produz material didático audiovisual, disponibilizado no canal do Youtube GaneshICMC[6], que conta com aulas, palestras e atividades que alimentam a curiosidade de jovens, adultos e crianças nos mais diversos assuntos da área de Segurança da Informação. Por fim, códigos fonte e arquivos de configuração de servidores dos CTFs, bem como respectivas soluções, são compartilhados no repositório público do Github[7], o que auxilia no entendimento de ferramentas usadas por profissionais da área e fornece formas de praticar programando e testando vulnerabilidades de segurança.

4.3 CTFs

O Grupo Ganesh[8] se destaca em competições de *Capture the Flag* (CTF) que testam conhecimento de Segurança da Informação por meio de desafios diversos como descriptografar dados ou explorar vulnerabilidades em serviços *Web*. Desde 2019, o grupo mantém uma posição sólida entre as melhores equipes do Brasil, inicialmente conquistando a 8ª posição no *ranking* brasileiro, e 5º lugar no ano seguinte. Durante o período de 2021 a 2023, o Ganesh manteve-se entre as três melhores equipes do país e a melhor equipe universitária. Segundo a plataforma *CTFtime*[9] que agrega pontuações de diversas competições de CTFs, em 2024 o Ganesh foi o melhor time do país e 184º do mundo. No ano atual, a disputa continua e o grupo atualmente está em primeiro lugar no *ranking* nacional e 32º no *ranking* global.

Portanto, os CTFs são ferramentas de aprendizado relevantes, que possibilitam a exploração de diferentes tipos de vulnerabilidades em diversos sistemas computacionais dentro de ambientes controlados. Dessa forma, a ideia é que ao aprender em ambientes simulados, o participante consiga identificar e relatar falhas em sistemas reais para que possam ser corrigidas antes de um atacante malicioso causar danos ao sistema [9].

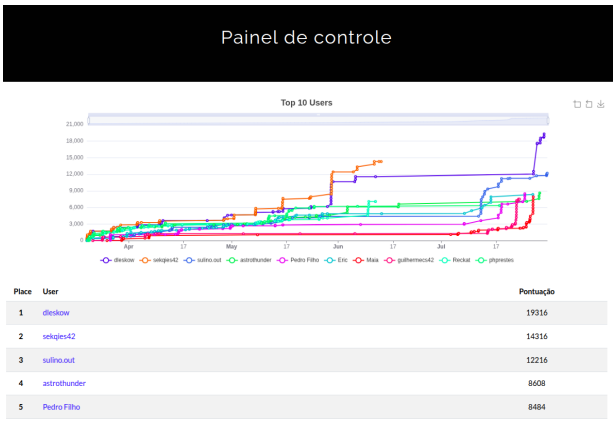
4.4 CTFd: um *framework Web* de ensino

O CTFd[10] é uma plataforma *Web* utilizada pelo grupo para propor desafios práticos voltados para o ensino dos temas abordados durante os cursos. Essa plataforma customizável e *open source* foi criada pela comunidade de Segurança da Informação como uma estratégia de ensino gamificada para engajar os estudantes. Nela, é possível criar desafios próprios com diferentes categorias de conhecimento, oferecer dicas durante os exercícios e disponibilizar desafios dinâmicos personalizáveis atribuindo diferentes pontuações. Uma abordagem interessante é que em alguns casos, a plataforma oferece a opção de os administradores oferecerem dicas conforme o participante conclua algumas tarefas. Ao longo do desafio, também é possível acompanhar as pontuações de todos os estudantes no desafio e avaliar o aprendizado de forma inovadora.

A plataforma foi utilizada inclusive no PING 2025[11] com desafios de Segurança da Informação para os ingressantes responderem e pontuarem conforme os acertos durante os exercícios. Foram 116 participantes no CTF do PING 2025, proporcionando uma experiência inicial engajadora para novos alunos e alunas presentes. Na Figura 7, é apresentado um *dashboard* personalizado com o desenvolvimento dos jogadores ao longo dos desafios do CTF.

A gamificação [8] surge como uma alternativa para o aprendizado de conceitos abstratos, como algoritmos de criptografia e protocolos de redes, que muitas vezes podem desencorajar os alunos em um primeiro contato. A partir dos conceitos e desafios iniciais,

[5] https://gitbook.ganeshicmc.com
[6] https://www.youtube.com/c/GaneshICMC
[7] https://github.com/ganesh-icmc
[8] https://ctf-br.org/wiki/ganesh
[9] https://ctftime.org/team/54706
[10] https://ctfd.io/
[11] https://ganesh.icmc.usp.br/ctf/scoreboard



Place	User	Pontuação
1	dleskow	19316
2	sekqles42	14316
3	sulino.out	12216
4	astrothunder	8608
5	Pedro Filho	8484

Figura 7: *Dashboard* oferecido pela plataforma CTFd representando a distribuição e o desempenho dos participantes do PING 2025 ministrado pelo Ganesh.

o participante consegue se engajar em desafios mais complexos individualmente ou muitas vezes em equipe.

Com isso, o uso do *CTFd* promove uma integração entre diferentes alunos do grupo, que se engajam na solução das tarefas e no aprendizado das vulnerabilidades encontradas nos desafios da plataforma. A hospedagem da plataforma de CTF, dos *websites* e outros serviços que fazem parte dos desafios foi proporcionada pela Superintendência de Tecnologia da Informação (STI) do ICMC.

4.5 Eventos e Workshops

Diante das iniciativas do grupo, o Ganesh começou sua trajetória no mundo das disputas das competições de CTFs, e também marcando presença em grandes eventos da comunidade brasileira e internacional de Segurança da Informação, como a *Hackers 2 Hackers Conference* (H2HC) [7] e a *DEFCON* [4].

A trajetória competitiva do grupo começou em 2019, quando alcançou a 8ª colocação no *ranking* brasileiro da plataforma *CTFtime*. Posteriormente, alcançou-se a 5ª colocação em 2020 e mantendo-se em 3º lugar entre 2021 e 2023. Já em 2024, obtiveram o melhor resultado, sendo reconhecidos como a melhor equipe do Brasil e da América Latina, figurando atualmente no grupo dos 150 melhores times do mundo entre mais de 37 mil times registrados [3]. Com isso, o Ganesh se consolidou como um projeto de influência no cenário de Segurança da Informação, sendo um dos principais grupos do país.

Uma trajetória marcante do grupo foi a participação no evento *Cyber Apocalypse* 2024, onde o Ganesh conquistou o 36º lugar entre mais de 3000 equipes, sendo a única equipe brasileira a ocupar as primeiras 500 posições. Esses resultados demonstram o engajamento dos estudantes e a dedicação em transformar a teoria, as aulas e o aprendizado em impactos práticos. O estudo colaborativo proposto com metodologias de desafios constantes e o engajamento em comunidade geram resultados expressivos na educação dos participantes.

Na Figura 8 é ilustrada a participação do grupo Ganesh formando a equipe "*Pwn* de Queijo" que enfrentou as eliminatórias da competição de CTF da conferência *DEFCON*, uma das competições de

Figura 8: Participação do time Ganesh nas qualificatórias da competição de CTF entre diferentes times ao redor do mundo da conferência internacional DEFCON.

Figura 9: Participação do Ganesh na competição de CTF da conferência H2HC na edição de 2024.

segurança mais prestigiadas do mundo. A equipe foi formada por Ganesh, "Boitatech" e "ELT". As competições e os desafios tiveram duração de 48 horas, com aproximadamente 20 desafios. A equipe alcançou a 17ª posição no *ranking* global, promovendo a integração das atividades e dos conhecimentos técnicos do Ganesh junto a diferentes equipes competitivas.

Outro evento em que o grupo Ganesh esteve presente foi a conferência H2HC (Figura 9). Diante de diferentes equipes, o grupo participou de desafios competitivos no formato de CTF e conquistou o 3º lugar.

5 RELATOS DOS ALUNOS E *FEEDBACKS*

Foram coletados dados via formulário sobre a satisfação de alguns dos cursos oferecidos. O curso de "Segurança defensiva para pessoas leigas (como não cair em golpes e baixar vírus)" teve um *feedback* positivo sobre o material apresentado. Algumas das mensagens dos alunos (M) no último dia de aula foram transcritas a seguir:

M1: "Adorei, equipe de parabéns, dinâmica muito clara. Ótimo curso, queria parabenizar a todos. Serão ótimos profissionais e ajudarão muito a sociedade na Segurança. Para melhoria no curso, seria melhorar a comunicação externa sobre o curso."

M2: "O material foi muito bem organizado. Em cada tópico vi algo que não tinha conhecimento. A equipe é muito simpática. Parabéns a todos os envolvidos!"

M3: "Descobri o curso pela FAPESP. Adorei! Sugiro apenas incluir formas práticas, com exemplos, de como gerir a privacidade e onde e como denunciar o descumprimento da LGPD."

Também foram coletados dados via formulário sobre o PING de 2025. Algumas das mensagens dos participantes (P) do PING deste ano foram transcritas abaixo:
P1: "Aula bem boa, meio densa, mas inevitável. Só gostaria de ter um pouco mais de demonstrações, mas entendo que o tempo foi curto, porém ainda foi uma aula bem proveitosa."
P2: "adorei a didática, sempre atenciosos com os alunos!"
P3: "Muito interessante, principalmente o funcionamento da criptografia OTP e o motivo pelo qual ela não é viável."
P3: "A aula foi super incrível! O uso de momentos mais dinâmicos como o *Kahoot* e a demonstração de *crib* deixam a aula muito mais interessante e fomentam bastante a participação dos ouvintes! Os conteúdos abordados são muito bons também! E, aproveitando a aula de hoje: *K Npetqp z ibdrzy*!."
P4: "Cai de paraquedas nesse conteúdo. *Youtube* me recomendou e curti muito a aula. Agradeço pelo vídeo ter ficado público. E parabéns ao apresentador e à equipe. Conteúdo excelente."

6 ÉTICA

Em todos os projetos do Ganesh, a participação do público é realizada de forma voluntária. Sendo assim, os participantes assinam um termo de Livre Consentimento para a participação nos projetos e minicursos. Além disso, os dados dos participantes, como por exemplo, *feedbacks* gerais, controle de presença e os desafios resolvidos apenas são utilizados para a melhoria dos cursos e atividades. Na plataforma *CTFd*, os usuários são identificados apenas por um "apelido" definido pelo próprio usuário, que não requer relação com o nome real, possibilitando participação completamente anônima daqueles que assim desejam. Portanto, nenhum dado em relação aos participantes é publicado e divulgado externamente pelo Ganesh.

7 CONSIDERAÇÕES FINAIS

Os cursos de extensão universitária exercem um papel essencial entre a universidade e a sociedade, oferecendo oportunidades de aprendizado contínuo e democratizando o acesso à educação, especialmente em áreas de destaque, como a Segurança da Informação. Mais do que atender à exigência de horas complementares, esse projeto, desde sua criação, promove a troca de experiências e a colaboração, adquirindo competências fundamentais para os desafios da sociedade atual. Ao longo dos anos, diversos docentes e estudantes da USP participaram do projeto Ganesh como coordenadores e monitores, colaborando na construção e no aprimoramento da metodologia adotada.

O principal propósito de um grupo de extensão é envolver a comunidade acadêmica e o público externo, e o Ganesh tem cumprido esse papel ao promover ações de impacto positivo disponibilizando materiais didáticos, trocando experiências e conhecimentos em eventos, além de realizar diversos cursos que promovem a disseminação de conteúdos técnicos de Segurança da Informação. Reconhecendo que a educação é um processo contínuo e em constante desenvolvimento, o projeto responde à crescente demanda por profissionais qualificados capazes de proteger sistemas e dados sensíveis em um mundo cada vez mais digitalizado. Além disso, o processo seletivo do PING é inclusivo, pois permite que todos participem, garantindo que qualquer pessoa interessada na área tenha acesso a uma educação de qualidade e gratuita, onde pode-se abrir possibilidades concretas no mercado de trabalho e na área acadêmica.

O projeto, dessa forma, contribui diretamente para a meta da Agenda 2030 da ONU relacionada à Educação de Qualidade, ao oferecer conhecimento técnico de forma inclusiva, acessível e transformadora. Espera-se que essa experiência sirva de inspiração para que outros grupos, de diferentes áreas possam criar conteúdos para propagar conhecimento a pessoas que possuem pouco acesso a informação, usando de plataformas de alto alcance, como o *YouTube*, *Gitbook*, *Instagram* para criação de conteúdo e divulgação de conteúdo e propósito educacional, reunir pessoas com interesses no conteúdo, como, por exemplo: via salas virtuais no *Google Meet* ou em encontros presenciais caso haja envolvimento com alguma universidade. Assim, estimulando um caminho pedagógico para que universidades ou grupos independentes implementem ações similares, ampliando o alcance da educação em Segurança da Informação e fortalecendo a cultura de proteção digital e educacional na sociedade.

8 AGRADECIMENTOS

Agradecemos a todos os alunos ingressantes e ex-alunos, de graduação e pós-graduação, que participaram do projeto. Deixamos registrado aqui também nosso agradecimento especial aos discentes envolvidos desde o início do projeto. Agradecemos também à Comissão de Cultura e Extensão (CCEx) do ICMC, à FAPESP, à CAPES e ao CNPq pelo apoio financeiro fornecido ao longo dos anos, e que viabilizou a realização dos cursos, eventos e outras iniciativas. Destacamos, por fim, que o grupo de autores deste trabalho representa um pequeno número de alunos e voluntários que passaram pelo curso ao longo desses anos.

REFERÊNCIAS

[1] BRASIL. 2018. Lei n. 13.709, de 14 de agosto de 2018. Diário Oficial da União. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Lei Geral de Proteção de Dados Pessoais (LGPD). Acesso em: 19 de agosto de 2025.
[2] CNN Brasil. 2025. *Vazamento expõe bilhões de senhas do Google, Apple e Meta, diz site.* https://www.cnnbrasil.com.br/tecnologia/vazamento-expoe-bilhoes-de-senhas-do-google-apple-e-meta-diz-site Acesso em: 18 ago. 2025.
[3] CTFtime.org. 2025. Ganesh – CTFtime.org. https://ctftime.org/team/54706/. Acesso em: ago. 2025.
[4] DEF CON. 2025. DEF CON Hacking Conference. https://defcon.org/. Acesso em: ago. 2025.
[5] G1. 2025. *Clientes do Neon têm dados vazados e banco alerta para tentativas de golpes.* https://g1.globo.com/economia/negocios/noticia/2025/02/12/clientes-do-neon-tem-dados-vazados-e-banco-alerta-para-tentativas-de-golpes.ghtml Acesso em: 18 ago. 2025.
[6] Michael Gleeson. 2024. Cybersecurity Students Experiences of Capture the Flag (CtF) in an Irish Technological University. In *2024 Cyber Research Conference - Ireland, Cyber-RCI 2024.* Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/Cyber-RCI60769.2024.10939974
[7] H2HC Conference. 2025. H2HC – Hackers to Hackers Conference. https://www.h2hc.com.br/. Acesso em: ago. 2025.
[8] María del Carmen Huamaní Quispe and Carlos Sixto Vega Vilca. 2023. Efectos de la gamificación en la motivación y el aprendizaje. *Horizontes. Revista de Investigación en Ciencias de la Educación* 7, 29 (April 2023), 1399–1410. https://doi.org/10.33996/revistahorizontes.v7i29.600
[9] Instituto de Ciências Matemáticas e de Computação (ICMC-USP). 2024. Grupo da USP alcança posição de destaque na América Latina em competições de cibersegurança. https://www.icmc.usp.br/noticias/6648-grupo-da-usp-alcanca-posicao-de-destaque-na-america-latina-em-competicoes-de-ciberseguranca Acesso em 18 de agosto de 2025.

[10] Janete Aparecida Klein, Carlos Eduardo da Silva, Janaina Santana da Costa, Eduardo Nunes Silva, Alessandra de Fátima Alves, Kyrleys Pereira Vasconcelos, Rodrigo Antonio Magalhães Teixeira, Emanuella Cruz Barbosa Vieira, Katia Maria Barros Leite, and Marcos André Trindade da Silva. 2025. CONECTADOS, MAS DEPENDENTES? REFLEXÕES SOBRE OS DILEMAS DA EDUCAÇÃO NA ERA DIGITAL. *ARACÊ* 7, 6 (2025), 32456–32474.

[11] Azah Anir Norman, Athirah Husna Marzuki, Fatokun Faith, Suraya Hamid, Norjihan Abdul Ghani, Sri Devi Ravana, and Noreen Izza Arshad. 2023. Technology Dependency and Impact During COVID-19: A Systematic Literature Review and Open Challenges. *IEEE Access* 11 (2023), 40741–40760. https://doi.org/10.1109/ACCESS.2023.3250770

[12] Sanjeev Parkar and Dharmesh K. Mishra. 2024. Cybersecurity Workforce Development and Training: A Comprehensive Review on the Significance, Strategies, Opportunities and Challenges. In *2024 International Conference on Intelligent Systems for Cybersecurity, ISCS 2024*. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ISCS61804.2024.10581241

[13] PUC-Campinas / CIESP. 2024. Presidente do Ciesp diz que o Brasil terá déficit de 140 mil profissionais de cibersegurança até 2025. https://www.puc-campinas.edu.br/presidente-do-ciesp-diz-que-o-brasil-tera-deficit-de-140-mil-profissionais-de-ciberseguranca-ate-2025/. Acesso em: 19 ago. 2025.