**Segurança Cibernética para Todos: Um Programa Educacional Interativo para Conscientização e Proteção Digital**

Fernanda Alves Fahl¹; Daniele Caroline Lima Da Silva²

1 MBA em Engenharia de Software – USP/Esalq

² Orientadora – USP/Esalq

**Segurança Cibernética para Todos: Um Programa Educacional Interativo para Conscientização e Proteção Digital**

**Resumo (ou Sumário Executivo)**

Este trabalho apresenta os resultados preliminares de uma pesquisa aplicada que visa desenvolver e implementar um programa educacional interativo e acessível em segurança cibernética, voltado para o público geral. O estudo parte da constatação de que a maioria das iniciativas educativas nessa área são voltadas a profissionais de TI, deixando de fora os usuários comuns, que também estão expostos a uma ampla gama de ameaças digitais. Com base em relatos coletados por meio de questionários, foram identificados os principais tipos de ameaças enfrentadas e os sentimentos mais recorrentes entre as vítimas. A abordagem educacional proposta será gamificada, com foco em vídeos e simulações práticas, visando alcançar públicos com diferentes estilos de aprendizagem e níveis de alfabetização digital. Os resultados iniciais confirmam a relevância e urgência do projeto, reforçando a necessidade de uma cultura digital inclusiva e segura.

**Palavras-chave:** segurança digital; educação; gamificação; conscientização; proteção de dados.

**Introdução**

No cenário digital contemporâneo, a segurança cibernética tornou-se uma preocupação urgente e universal. Com o crescimento exponencial do uso de dispositivos conectados e a digitalização de serviços pessoais, financeiros e sociais, indivíduos comuns estão cada vez mais expostos a riscos como roubo de identidade, golpes digitais, infecção por malware e vigilância não autorizada. No entanto, a maior parte das iniciativas educacionais existentes em segurança da informação é voltada para profissionais técnicos ou estudantes da área, ignorando a vulnerabilidade de um público mais amplo e leigo.

Segundo Schneier (2015), vivemos na "era dourada da vigilância", em que governos e corporações coletam e utilizam dados pessoais de forma invisível e massiva. Anderson (2020) argumenta que falhas de segurança também decorrem de falhas humanas e da ausência de soluções que priorizem a usabilidade. Stallings e Brown (2018) reforçam a necessidade de todos os usuários compreenderem os princípios fundamentais da segurança da informação — confidencialidade, integridade e disponibilidade — como pré-requisito para o uso consciente da tecnologia.

Diante desse contexto, este trabalho busca promover a alfabetização digital crítica por meio de um programa educacional acessível, interativo e gamificado, direcionado a pessoas sem formação técnica, com o objetivo de construir uma cultura de segurança digital inclusiva e replicável. Para isso, o projeto adota uma abordagem inspirada no Design Thinking, uma metodologia que valoriza a empatia com o usuário, a experimentação e a iteração contínua como formas de encontrar soluções centradas nas pessoas.

De acordo com Ambrose e Harris (2015), o design deve ser entendido como um processo que vai além da estética, englobando a criação de experiências significativas que atendem às necessidades reais dos usuários.

O site educacional que sustenta este programa foi concebido com base nos princípios do Domain Driven Design (DDD), que busca alinhar o desenvolvimento de software com a lógica do domínio específico em que ele será aplicado. Ao focar na linguagem ubíqua, em contextos delimitados e em regras de negócio específicas, o DDD permite criar sistemas que realmente refletem a realidade dos usuários finais e favorecem a comunicação entre desenvolvedores e especialistas do domínio.

No caso deste projeto, os domínios identificados foram organizados em trilhas temáticas como “Defesa Pessoal Digital”, “Golpes e Trapaças” e “Compras com Segurança”, com base nas principais ameaças relatadas por usuários em um levantamento prévio.

A experiência de uso da plataforma foi projetada de forma a ser simples, fluida e emocionalmente envolvente. O design visual segue diretrizes de usabilidade e acessibilidade, com interface clara, linguagem não técnica e recursos visuais lúdicos. A gamificação entra como elemento estratégico de engajamento: o conteúdo é apresentado por meio de simulações, quizzes e microdesafios, acompanhados de um sistema de recompensas simbólicas. Isso se apoia na ideia de que jogos são ambientes seguros para errar, experimentar e aprender — e que, ao promoverem feedbacks imediatos, aumentam a retenção de conhecimento e a motivação do usuário.

O desenvolvimento da plataforma também foi influenciado pelos princípios da Arquitetura Limpa, que preza pela separação entre regras de negócio e aspectos técnicos, garantindo um sistema mais testável, escalável e fácil de manter.

Dessa forma, a estrutura do projeto visa a durabilidade da solução e a possibilidade de expansão futura com novas trilhas e funcionalidades.

Este relatório apresenta os resultados preliminares de uma pesquisa que investigou o conhecimento, comportamentos e percepções de usuários comuns frente a riscos digitais. Esses dados foram fundamentais para a definição do escopo funcional e pedagógico da plataforma, permitindo o desenvolvimento de uma solução verdadeiramente orientada ao usuário.

**Metodologia ou Material e Métodos**

Esta pesquisa caracteriza-se como exploratória, de natureza aplicada, com abordagem mista (qualitativa e quantitativa). Seu objetivo central é investigar a percepção de usuários comuns sobre segurança digital e, a partir dos dados levantados, desenvolver um programa educacional interativo e gamificado que promova práticas seguras no uso cotidiano de tecnologias.

A escolha pela abordagem exploratória se justifica pelo caráter ainda pouco sistematizado do tema no que diz respeito à educação voltada para leigos, especialmente no Brasil. A proposta não é validar hipóteses previamente estabelecidas, mas entender comportamentos, sentimentos e padrões de aprendizado de usuários diante de ameaças digitais reais, e usar esse entendimento para construir soluções práticas e acessíveis.

Coleta de Dados

Foi aplicado um questionário online para 107 participantes anônimos e voluntários, composto por perguntas abertas e fechadas, distribuído por meio de redes sociais e grupos diversos de usuários. A estratégia de coleta visou alcançar um público heterogêneo, sem formação técnica obrigatória, de forma a capturar diferentes níveis de familiaridade com tecnologia e segurança digital.

As perguntas fechadas foram formuladas para quantificar:

* Frequência de exposição a ameaças (ex: invasão de contas, golpes financeiros);
* Tipos de serviços digitais utilizados;
* Conhecimento prévio de práticas de segurança (uso de senhas fortes, autenticação em dois fatores);
* Estilos de aprendizado preferidos (vídeos, leitura, prática, etc.).

Já as perguntas abertas foram essenciais para captar:

* Relatos pessoais de incidentes e golpes sofridos;
* Reações emocionais (como medo, vergonha, impotência ou raiva);
* Barreiras percebidas para adotar comportamentos mais seguros.

Essa combinação de técnicas permitiu mapear tanto o “o que” (dados objetivos) quanto o “como” e o “porquê” (dimensões subjetivas e afetivas) das experiências dos participantes.

*Justificativa das Perguntas*

As perguntas foram elaboradas com base em princípios de segurança digital propostos por Stallings e Brown (2018) (confidencialidade, integridade e disponibilidade), e em discussões levantadas por Schneier (2015) e Anderson (2020) sobre vulnerabilidades humanas e estruturais. A intenção era compreender não apenas os ataques sofridos, mas como os usuários reagem emocionalmente a eles, e quais obstáculos enfrentam para adotar práticas mais seguras.

Além disso, as perguntas sobre estilo de aprendizagem preferencial foram incluídas como base para o design pedagógico da plataforma educacional, permitindo alinhar o conteúdo ao modo como os usuários de fato aprendem: com vídeos, simulações práticas, leitura ou tutoriais interativos.

*Análise dos Dados*

Os dados foram analisados por meio de uma abordagem mista, integrando:

* Análise estatística simples (quantitativa) para categorização e frequência dos eventos relatados;
* Análise de conteúdo temática (qualitativa) nas respostas abertas, com agrupamento em categorias como:
  + Invasão de contas,
  + Phishing e engenharia social,
  + Fraudes financeiras,
  + Reações emocionais pós-incidente,
  + Medidas adotadas após o ataque.

As categorias emergiram de forma indutiva, conforme a leitura recorrente dos relatos, permitindo identificar padrões relevantes para o projeto da solução educacional.

*Aplicação dos Resultados*

Os dados serviram como insumo direto para o desenvolvimento do programa educacional gamificado, estruturado com base em princípios de design centrado no usuário. A organização dos módulos reflete os domínios temáticos mais relevantes (como golpes online e compras seguras), e os recursos de gamificação foram escolhidos para refletir os estilos de aprendizagem mais populares entre os respondentes.

O processo de modelagem da plataforma está sendo conduzido com base nos princípios do Domain Driven Design (DDD), permitindo alinhar a linguagem de implementação com os conceitos emergentes da pesquisa (como “trilha”, “desafio”, “ameaça” e “reação”). Além disso, o uso de design thinking como abordagem orientadora tem garantido que o sistema não apenas resolva um problema técnico, mas crie uma experiência significativa e transformadora para o usuário.

**Resultados Preliminares**

A análise preliminar dos dados coletados revelou uma diversidade de ameaças digitais enfrentadas por usuários comuns, mesmo entre aqueles com pouca familiaridade técnica. Os incidentes foram agrupados em oito categorias principais:

1. Invasão de Contas: Relatos frequentes de acessos indevidos em redes sociais, e-mails, plataformas de jogos e serviços de streaming. As consequências incluíram perda de acesso, golpes aplicados por terceiros e redefinição forçada de senhas.
2. Infecção por Vírus e Malware: Associada ao download de softwares suspeitos ou piratas. Houve registro de perda de dados e comprometimento de dispositivos pessoais.
3. Golpes de Phishing e Engenharia Social: Envolvendo mensagens falsas, sites falsificados e tentativas de coleta de dados pessoais. Foram relatadas fraudes via WhatsApp, e-mail e redes sociais, muitas vezes resultando em prejuízos ou vazamento de dados sensíveis.
4. Fraudes em Compras Online: Compras não entregues, perfis falsos em marketplaces e dificuldades de reembolso foram recorrentes. Tais experiências evidenciam a falta de checagem de autenticidade de vendedores e a vulnerabilidade a golpes estruturados.
5. Clonagem e Uso Indevido de Cartões: Incluindo clonagem de cartões físicos e virtuais, com uso não autorizado detectado após transações suspeitas. Muitos participantes relataram estornos bancários e bloqueios de cartão.
6. Vazamento de Dados Pessoais: Diversos participantes perceberam que seus dados (CPF, telefone, e-mail, etc.) estavam disponíveis publicamente ou foram utilizados por terceiros sem consentimento.
7. Golpes via Aplicativos e Dispositivos Comprometidos: Casos de perfis clonados em aplicativos de mensagens e invasões em dispositivos móveis demonstram a necessidade de segurança ampliada para o uso cotidiano.
8. Falhas por Falta de Informação: Uso da mesma senha em diversos serviços, ausência de autenticação em dois fatores e desconhecimento de recursos de segurança bancária foram citados como fatores contribuintes para ataques.

Além dos aspectos técnicos, os resultados revelam uma dimensão emocional importante. Sentimentos como frustração, vergonha e impotência foram citados com frequência por vítimas de golpes digitais. Alguns participantes destacaram a sensação de terem sido enganados por sua própria ingenuidade, enquanto outros relataram que passaram a adotar hábitos mais seguros após o ocorrido.

Quanto aos métodos de aprendizagem preferidos, a maioria apontou o uso de vídeos no YouTube como principal meio de aprendizado digital (63 respostas), seguido por leitura de artigos e textos (33), prática direta e cursos rápidos. Esse dado valida a escolha da metodologia interativa do programa, baseada em vídeos, simulações práticas e gamificação.

Esses resultados reforçam a relevância da proposta deste projeto e fornecem diretrizes claras para o desenvolvimento dos módulos educacionais. As ameaças identificadas, aliadas ao perfil de aprendizado do público, indicam a necessidade de um conteúdo claro, acessível e tecnicamente fundamentado, alinhado aos princípios de Stallings (2018), Schneier (2015) e Anderson (2020).

**Conclusão(ões) ou Considerações Finais**

Os resultados preliminares reforçam a necessidade de iniciativas educativas voltadas ao público leigo, com ênfase na compreensão de ameaças digitais e práticas de proteção cotidianas. A diversidade de ataques relatados e os danos emocionais descritos evidenciam que a segurança digital deve ser tratada como um direito fundamental e uma competência básica da cidadania contemporânea. O programa proposto pretende ser uma ferramenta eficaz de inclusão e empoderamento digital, contribuindo para uma sociedade mais segura e informada.

**Referências**

ANDERSON, R. *Security Engineering: A Guide to Building Dependable Distributed Systems*. 3. ed. Wiley, 2020.

AMBROSE, G.; HARRIS, P. *Design Thinking*. Brookman: Porto Alegre, RS, Brasil, 2015.

BROWN, T. *Design Thinking: Uma metodologia poderosa para decretar o fim das velhas ideias*. Rio de Janeiro: Alta Books, 2017.

MARTIN, R. C. *Arquitetura Limpa: O guia do artesão para estrutura e design de software*. Rio de Janeiro: Alta Books, 2019.

SCHNEIER, B. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton & Company, 2015.

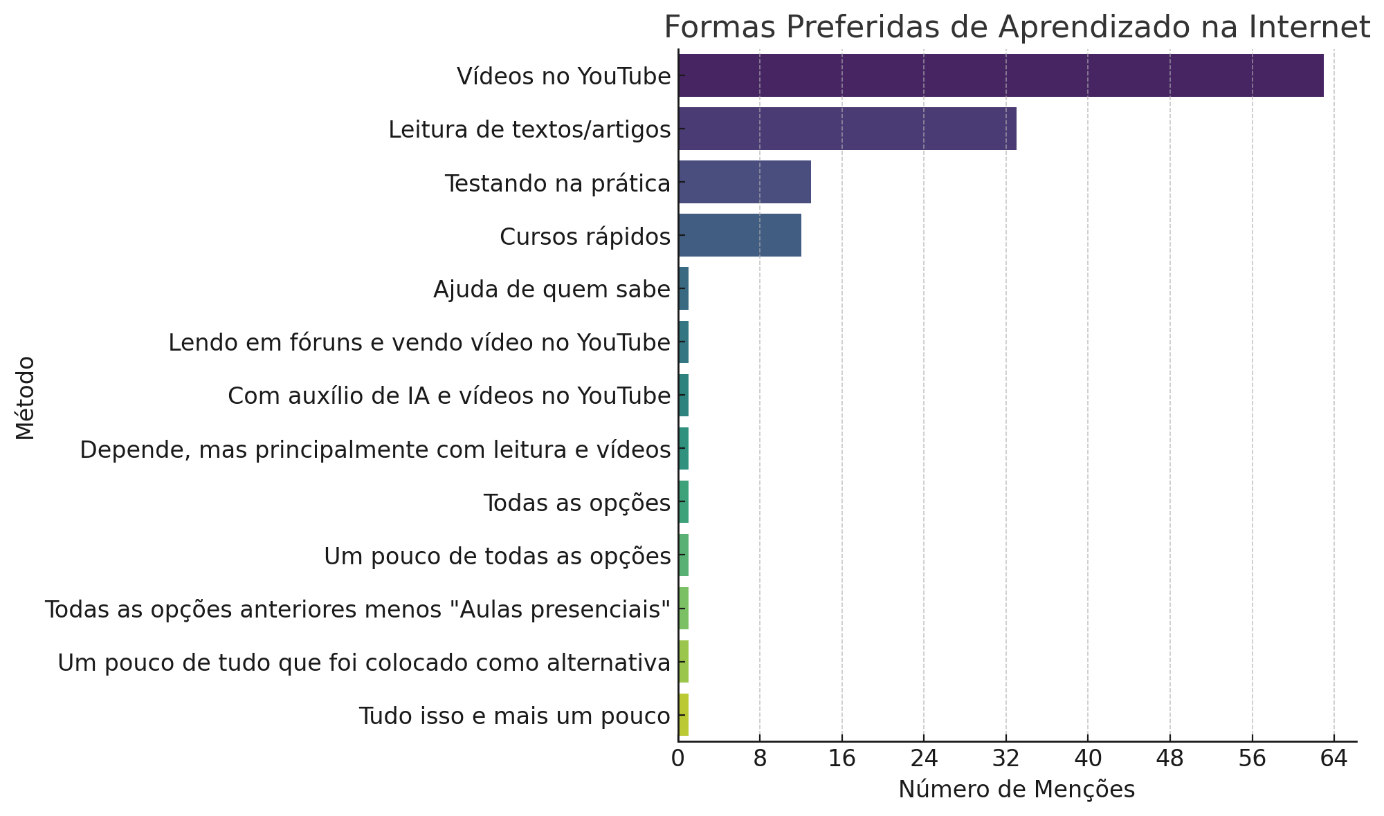
STALLINGS, W.; BROWN, L. *Computer Security: Principles and Practice*. 4. ed. Pearson, 2018.

**Apêndice ou Anexo**

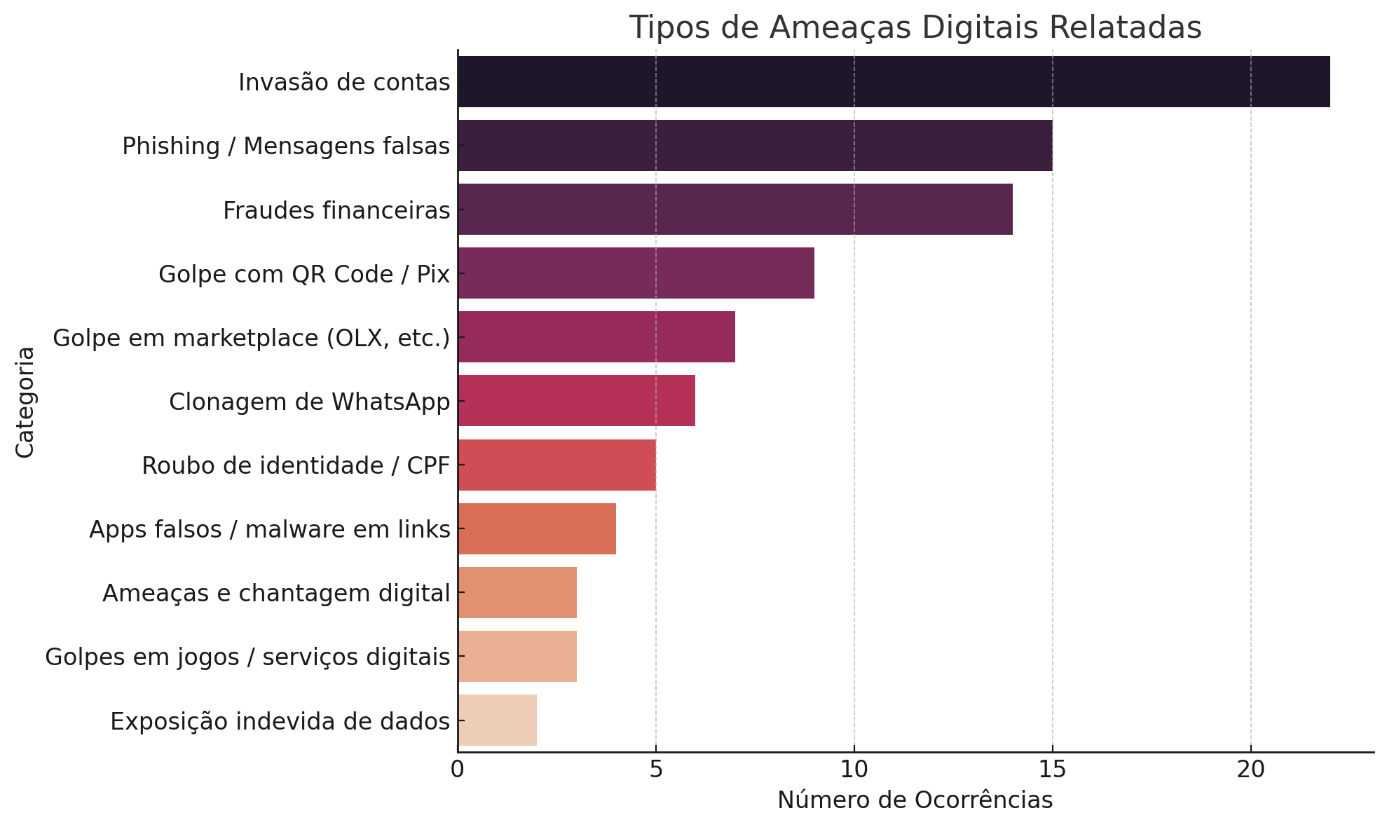
**APÊNDICE A — Categorização dos Incidentes Relatados pelos Participantes**

|  |  |  |
| --- | --- | --- |
| Tipo de Ameaça | Frequência Estimada | Exemplos de Relatos |
| Invasão de contas | Alta | “Perdi o acesso ao meu Instagram.” / “Usaram meu e-mail para aplicar golpes.” |
| Infecção por malware | Média | “Baixei um programa pirata e perdi todos os dados.” |
| Phishing e engenharia social | Alta | “Cliquei em um link de promoção e roubaram meus dados.” |
| Fraudes em compras online | Alta | “Comprei num site falso e nunca recebi o produto.” |
| Clonagem de cartões | Média | “Detectei compras que não reconhecia no meu cartão.” |
| Vazamento de dados pessoais | Média | “Meus dados estavam públicos em um site de verificação.” |
| Golpes por aplicativos | Média | “Clonaram meu WhatsApp e pediram dinheiro a meus contatos.” |
| Falta de conhecimento | Média | “Não sabia que podia ativar autenticação de dois fatores.” |

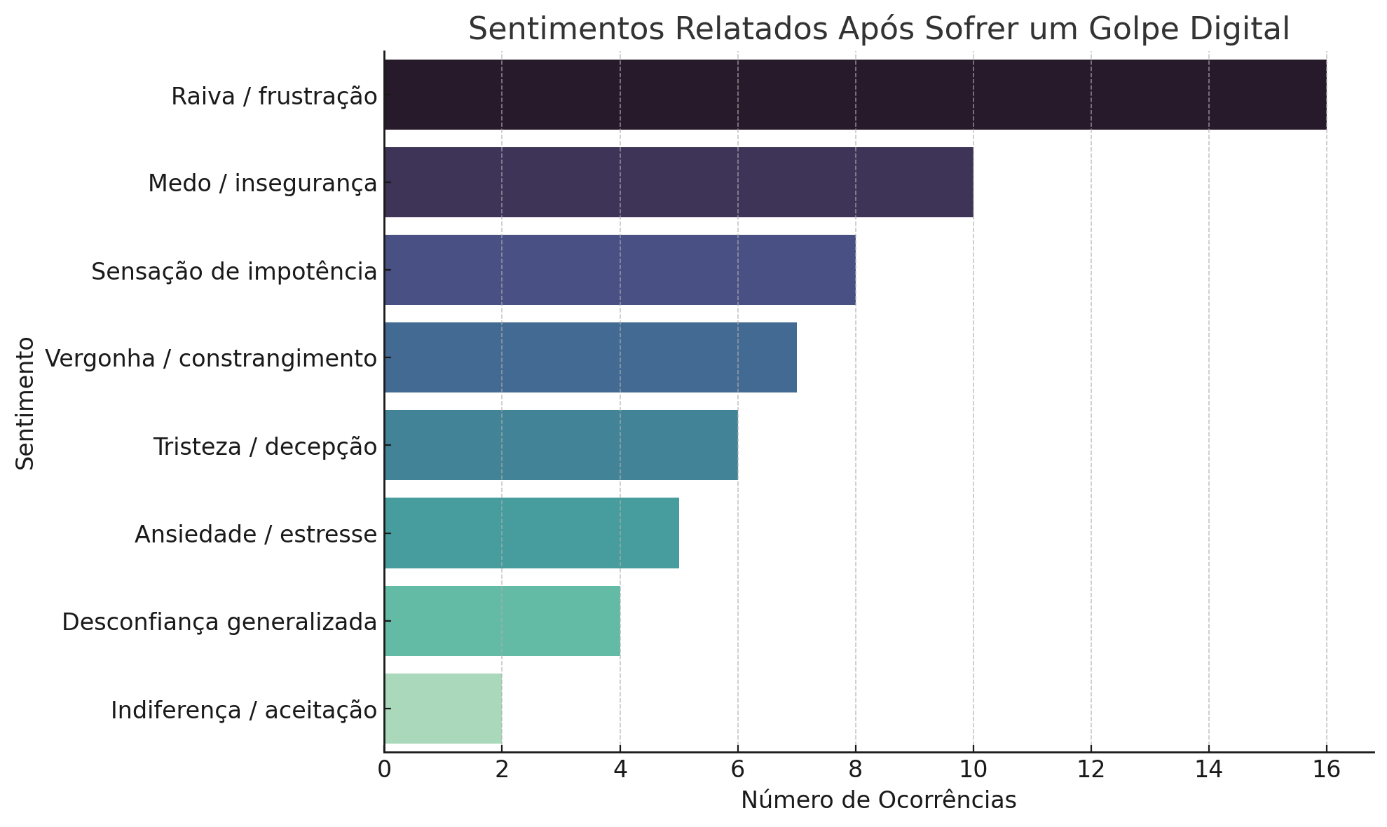
**APÊNDICE B — Formas Preferidas de Aprendizado na Internet**



**APÊNDICE C — Tipos de Ameaças Digitais Relatadas**



**APÊNDICE D — Sentimentos Relatados Após Experiências com Golpes**



**APÊNDICE E – Perfil dos Participantes da Pesquisa**

Este apêndice apresenta a análise do perfil dos respondentes do questionário “Segurança Digital no Dia a Dia”. As informações incluem:

* Familiaridade tecnológica: predominância de participantes com familiaridade média ou alta com tecnologia.
* Atuação na área: uma parte considerável trabalha ou estuda em áreas relacionadas à tecnologia.
* Busca por aprendizado: a maioria declara buscar frequentemente aprender sobre tecnologia, o que favorece ações educativas.
* Faixa etária: prevalência de participantes entre 18 a 44 anos, uma faixa bastante ativa online.
* Dispositivo de acesso: computador e celular se alternam como principais meios de acesso à internet.
* Acesso à internet: quase todos afirmam ter acesso constante à internet, reforçando a viabilidade de ações digitais**.**

**ANEXO A — Instrumento de Coleta de Dados (Questionário)**

Pesquisa: Segurança Digital no Dia a Dia

Objetivo: Entender como você usa a internet, quais são suas principais dúvidas e como podemos te ajudar a se proteger melhor no ambiente digital.

As suas respostas são anônimas e vão nos ajudar a criar um programa educacional gratuito e acessível para todos.

🧩 1. Perfil do Participante

1.1 Qual seu nível de familiaridade com tecnologia?

( ) Muito alto — trabalho ou estudo na área

( ) Médio — uso bastante no dia a dia, mas sem formação

( ) Baixo — uso o básico e tenho dificuldades às vezes

( ) Muito baixo — tenho bastante dificuldade com tecnologia

1.2 Você já estudou ou trabalha com informática, tecnologia ou segurança digital?

( ) Sim

( ) Não

1.3 Com que frequência você tenta aprender coisas novas sobre tecnologia?

( ) Frequentemente

( ) Às vezes

( ) Raramente

( ) Nunca

1.4 Quantos anos você tem?

( ) Menos de 18

( ) 18 a 29

( ) 30 a 44

( ) 45 a 59

( ) 60 ou mais

1.5 Com qual dispositivo você mais acessa a internet?

( ) Celular

( ) Computador

( ) Tablet

( ) Outro: \_\_\_\_\_\_\_\_\_\_\_\_

1.6 Você tem acesso fácil à internet?

( ) Sim, o tempo todo

( ) Sim, mas só com Wi-Fi em casa

( ) Não tenho acesso fácil

🔐 2. Experiência e Segurança Digital

2.1 Você já teve algum problema com segurança digital?

(Ex: conta invadida, golpe online, vírus, roubo de dados, etc.)

( ) Sim

( ) Não

( ) Não sei dizer

2.2 Se sim, o que aconteceu?

(Resposta aberta)

2.3 Você costuma criar senhas diferentes para cada conta online?

( ) Sim

( ) Não

( ) Às vezes

( ) Não sei como fazer isso

2.4 Você já recebeu mensagens suspeitas por e-mail, WhatsApp ou redes sociais?

( ) Sim, várias vezes

( ) Sim, algumas vezes

( ) Não tenho certeza

( ) Nunca

2.5 Você sabe o que é um “vírus” ou “malware” e como se proteger?

( ) Sim

( ) Não

( ) Já ouvi falar, mas não entendo bem

😨 3. Preocupações e Medos Online

3.1 Qual dessas situações mais te preocupa na internet?

(Marque as que quiser)

[ ] Ter dados pessoais roubados

[ ] Ter a conta bancária invadida

[ ] Perder o acesso às redes sociais

[ ] Cair em golpes financeiros

[ ] Baixar vírus sem saber

[ ] Outra: \_\_\_\_\_\_\_\_\_\_\_\_

3.2 Você já deixou de usar um site ou aplicativo por medo de segurança?

( ) Sim

( ) Não

( ) Já pensei nisso, mas usei mesmo assim

3.3 Você já caiu em algum golpe digital? Como se sentiu?

(Resposta aberta)

📘 4. Hábitos e Aprendizado

4.1 Você atualiza seus dispositivos e aplicativos com frequência?

( ) Sim

( ) Às vezes

( ) Não

( ) Não sei como fazer isso

4.2 Você verifica se um site é confiável antes de comprar algo online?

( ) Sim

( ) Às vezes

( ) Não

( ) Nunca comprei online

4.3 Como você costuma aprender algo novo na internet?

( ) Vídeos no YouTube

( ) Leitura de textos/artigos

( ) Cursos rápidos

( ) Aulas presenciais

( ) Testando na prática

( ) Outro: \_\_\_\_\_\_\_\_\_\_\_\_

🚀 5. Interesse e Engajamento

5.1 Você se interessaria por um curso rápido e gratuito sobre segurança digital?

( ) Sim

( ) Talvez

( ) Não

5.2 Qual formato de aprendizado mais te atrai?

( ) Vídeos curtos

( ) Textos simples com imagens

( ) Jogos educativos

( ) Aulas presenciais

( ) Outro: \_\_\_\_\_\_\_\_\_\_\_\_

5.3 Você se sentiria mais motivado(a) a participar se recebesse um certificado no final?

( ) Sim

( ) Talvez

( ) Não

5.4 Você participaria de jogos ou simulações práticas para aprender mais sobre segurança digital?

( ) Sim

( ) Talvez

( ) Não