Cibersegurança na Amazônia Legal: Mitigando Assimetrias de Proteção com CIS Controls IG1 e Conformidade com a Lei Geral de Proteção de Dados (LGPD)

Saymon Davidson Lima de Miranda[1] **, Rodrigo Brendo Miranda da Costa**[1]
Ynis Cristine de Santana Martins Lino Ferreira[1]

Instituto Ciberespacial – Universidade Federal Rural da Amazônia (UFRA)
Av. Presidente Tancredo Neves, Nº 2501 – CEP: 66.077-830 – Belém-Pará-Brasil

{saymon.miranda,rodrigobrendolc}@gmail.com, ynis.cristine@ufra.edu.br

Abstract. *This paper reports a case study and action research on CIS Controls IG1 in an OSCIP with 75 units in the Brazilian Legal Amazon. A mixed-methods intervention combined Bitdefender GravityZone and GoPhish. The deployment covered 255 endpoints and neutralized over 500 threats. Phishing simulations after awareness training showed a 34% interaction rate. The IG1 profile achieved 82% adherence to essential practices at a cost of BRL 26.21 per user per year. The results indicate that IG1 can improve cybersecurity maturity and support LGPD-aligned safeguards.*

Resumo. *Este artigo apresenta um estudo de caso e Pesquisa-Ação sobre a implementação dos CIS Controls IG1 em uma OSCIP com 75 unidades na Amazônia Legal. A intervenção combinou Bitdefender GravityZone e GoPhish. Foram protegidos 255 endpoints e neutralizadas mais de 500 ameaças. Após campanha de conscientização, as simulações de phishing registraram 34% de interação. O perfil IG1 alcançou 82% de aderência às práticas essenciais, com custo estimado de R$ 26,21 por usuário ao ano. Os resultados indicam que o IG1 pode elevar a maturidade de cibersegurança e apoiar salvaguardas alinhadas à LGPD.*

1. Introdução

A expansão do uso de tecnologias da informação nas organizações trouxe ganhos operacionais, mas também ampliou os riscos associados à segurança cibernética. Nesse contexto, organizações de menor porte e entidades do terceiro setor têm se tornado alvos recorrentes de ciberataques, pois frequentemente combinam ativos informacionais sensíveis com estruturas limitadas de defesa. Esse é o cenário da organização analisada, uma Organização da Sociedade Civil de Interesse Público (OSCIP) com 75 unidades distribuídas na Amazônia Legal, responsável pela gestão de dados sensíveis e pela administração de convênios bancários críticos, operando com orçamento restrito e equipe de tecnologia de informação reduzida. Embora juridicamente pertencente ao terceiro setor, sua dependência operacional de sistemas de informação a aproxima, do ponto de vista tecnológico e de gestão de riscos, de uma Pequena ou Média Empresa (PME).

Estudos atuais mostram que as PME são atacadas com frequência superior à de grandes corporações justamente por contarem com menos camadas de proteção,

políticas incipientes de segurança e programas frágeis de capacitação de usuários [Verizon Business 2025, Deloitte 2021, Duarte and Rizo 2024]. No cenário pesquisado, o diagnóstico inicial mostrou um ambiente de alta exposição: firewall ausente de perímetro, disseminação do uso de softwares não licenciados, falta de inventário sistemático de ativos e histórico de incidências, incluindo comprometimento de estação da diretoria com fraude bancária não rastreável e campanhas de phishing bem-sucedidas, servindo muitas vezes como elo mais fraco na cadeia de segurança [Federação do Comércio do Estado de São Paulo 2024, Kaspersky 2023, Segal 2022]. Em termos de maturidade, a instituição operava com respostas improvisadas de forma predominante e processos *ad hoc*, alinhando-se ao nível mais baixo dos modelos de referência, como o do National Institute of Standards and Technology(NIST).

Simultaneamente, migrar para os serviços em nuvem e o trabalho remoto ajudaram a dissolver o perímetro tradicional de rede [Nakamura and Geus 2007, CERT.br 2020], alterando a defesa para os dispositivos finais. Sem um perímetro físico com controle, a segurança torna-se dependente da proteção de *endpoints* e da autenticação de usuários, o que transforma o computador do colaborador na última linha de defesa contra ameaças. Nesse contexto, frameworks práticos como o CIS Controls, em sua versão 8, mostram um roteiro de priorização de controles capaz de traduzir boas práticas em ações técnicas viáveis para organizações com poucos recursos.

Diante desse contexto, este trabalho busca responder à seguinte questão: como implementar, de forma eficaz e economicamente viável, controles de segurança cibernética baseados no CIS Controls IG1 em uma infraestrutura de TI compacta e com recursos limitados de uma organização, a fim de, proteger ativos e dados e atender às exigências da Lei Geral de Proteção de Dados (LGPD) [Brasil 2018]? O objetivo geral é implementar e avaliar os Controles CIS v8, com foco no Grupo de Implementação 1 (IG1), como estratégia para elevar a maturidade de cibersegurança e o nível de compliance da instituição. Especificamente, busca-se: (i) diagnosticar a maturidade em segurança da informação; (ii) aplicar medidas de higiene cibernética com gestão unificada de *endpoints*; (iii) medir a suscetibilidade a ataques de engenharia social por meio de simulações de phishing; e (iv) propor diretrizes de conformidade compatíveis com as restrições financeiras e operacionais da organização.

2. Referencial Teórico

2.1. Segurança da informação e cibersegurança em PMEs

A segurança da informação concentra-se na proteção estratégica de ativos contra acessos não autorizados, alterações indevidas e interrupções operacionais, estruturada pela tríade *Confidencialidade, Integridade e Disponibilidade* (CIA) [Machado 2014]. A violação dos pilares da CIA pode acarretar em perdas financeiras expressivas, assim, afetando a credibilidade institucional. Com o aumento crescente da digitalização de processos e a hiperconectividade, a cibersegurança emergiu como especialização voltada à proteção de redes e ativos digitais em ambientes dinâmicos e hostis, incluindo práticas de prevenção, detecção e resposta a incidentes [Stallings and Brown 2014].

No contexto das PMEs, a aplicação integral de frameworks bem construídos, frequentemente, esbarra em restrições de orçamento e redução de equipes, levando

essas organizações a tratar segurança de forma reativa, o que as torna vetores convenientes para atacantes de baixo esforço [Deloitte 2021, Verizon Business 2025, Duarte and Rizo 2024].

2.2. CIS Controls v8 e Grupos de Implementação

O CIS Controls, mantido pelo Center for Internet Security, é um conjunto de 18 controles prescritivos e priorizados de melhores práticas de cibersegurança, concebido para traduzir recomendações em ações técnicas de execução [Center for Internet Security 2021]. Sua proposta possui um diferencial comparado à frameworks como a ISO 27001, que buscam enfatizar arcabouços documentais amplos; o CIS Controls adota abordagem prática, voltada à mitigação dos vetores de ataque mais prevalentes.

A versão 8 introduz os Grupos de Implementação (IGs) para tornar viável a adoção gradual, proporcionalmente ao perfil de risco e à capacidade de operação de cada instituição. O IG1, denominado "Higiene Cibernética Essencial", é voltado a organizações com recursos limitados e pessoal de TI generalista, privilegiando salvaguardas que impedem ataques automatizados e com teor oportunista, além de, abranger 56 salvaguardas distribuídos entre os 18 controles do framework. Não representa a opção de "menor segurança", mas sim a construção de um alicerce técnico estruturado antes de avançar para controles mais complexos. A organização analisada foi colocada nesse perfil, dado que combina dependência de hardware e software comerciais com forte restrição orçamentária e equipe de TI compacta [Center for Internet Security 2021].

2.3. Fator humano, engenharia social e literacia digital

Independentemente da sofisticação das barreiras tecnológicas, o fator humano permanece um dos principais vetores explorados em ataques cibernéticos [Mitnick and Simon 2003]. A literatura clássica em engenharia social mostra que manipular de forma psicológica um colaborador costuma ser mais satisfatório para um atacante do que tentar quebrar mecanismos de criptografia, principalmente quando não existe uma cultura de segurança organizacional consolidada.

Técnicas como *spear phishing* e *brand impersonation*,responsáveis por simular notificações de plataformas conhecidas como Google ou Microsoft, exploram gatilhos de urgência para induzir ações impulsivas, como clicar em links maliciosos ou fornecer dados em páginas fraudulentas [Barracuda Networks 2022]. Relatórios de ameaças mostram que colaboradores de organizações pequenas são, em média, muito mais expostos a esse tipo de ataque do que profissionais de corporações maiores, em razão de menor treinamento e controles menos rigorosos [Barracuda Networks 2022, Segal 2022].

Nesse cenário, o Controle 14 do CIS, dedicado a conscientização e treinamento em segurança, mostra-se como peça central de qualquer estratégia de defesa. Pesquisas apontam que programas contínuos de simulação e capacitação são capazes de atuar na transformação de colaboradores em agentes ativos de defesa, aumentando a percepção de risco e reduzindo a taxa de interação com conteúdos maliciosos [Kanagusku and Gaseta 2023].

2.4. LGPD, compliance e continuidade de negócios

A Lei Geral de Proteção de Dados Pessoais (LGPD), em seu Artigo 46, exige que controladores e operadores adotem medidas técnicas e de cunho administrativo capazes de

proteger dados pessoais contra acessos não autorizados, perda, destruição ou alteração [Brasil 2018]. O Artigo 50, por sua vez, estimula a adoção de boas práticas e de programas de governança focados em privacidade, incluindo mecanismos de *accountability*, ou seja, a capacidade de mostrar evidências concretas das medidas implementadas [Fontes and Truzzi 2020].

Nesse quadro, frameworks técnicos como os CIS Controls assumem papel instrumental: a implantação dos controles não apenas aumenta a maturidade de segurança, mas também cria registros e relatórios que operacionalizam o dever legal de proteção de dados. A literatura sobre incidentes de *ransomware* em organizações brasileiras indica que os impactos de uma falha de segurança vão além do aspecto técnico, atingindo a viabilidade financeira, a capacidade de manutenção de empregos e a reputação junto a parceiros e usuários [Menchão et al. 2024].

Para PMEs e organizações do terceiro setor que prestam serviços de interesse público, essa convergência entre controles técnicos, conformidade legal e continuidade operacional é preocupante: um incidente de segurança pode comprometer não apenas sistemas internos, mas também, a prestação de serviços dependentes de convênios e parcerias institucionais.

3. Metodologia

3.1. Abordagem de pesquisa

A investigação foi conduzida como um Estudo de Caso de natureza aplicada[Yin 2015], articulado à Pesquisa-Ação, com abordagem mista (qualitativa e quantitativa). O Estudo de Caso permitiu analisar com profundidade o fenômeno da cibersegurança em uma OSCIP com características de PME, tendo em consideração o seu contexto organizacional, tecnológico e regulatório. A Pesquisa-Ação priorizou a intervenção planejada no ambiente, em cooperação com a equipe de TI e gestores, possibilitando de modo simultâneo, resolver problemas práticos e produzir evidências empíricas [Thiollent 2011].

3.2. Contexto, participantes e instrumentos

O estudo foi realizado em uma organização do terceiro setor com 75 unidades distribuídas na Amazônia Legal e aproximadamente 500 usuários administrativos e operacionais. A infraestrutura de TI era composta por estações de trabalho heterogêneas, conectadas à internet por provedores locais, sem VPN com a matriz e sem firewall de perímetro padronizado. Das aproximadamente 500 pessoas que utilizam recursos tecnológicos na organização, 255 foram priorizadas para a implantação das licenças de proteção de *endpoint* por corresponderem aos usuários administrativos com acesso direto a sistemas críticos, como plataformas bancárias, arquivos de convênios e dados pessoais sob escopo da LGPD, em conformidade com o critério de priorização por risco previsto no próprio IG1; os demais usuários operacionais usam dispositivos móveis ou terminais compartilhados sem acesso a esses sistemas, sendo contemplados em fases posteriores da implantação.

Foram utilizados três conjuntos principais de instrumentos:

3.3. Etapas do estudo

O percurso metodológico foi estruturado em três etapas sequenciais e complementares.

Tabela 1 - Instrumentos aplicados no estudo

Instrumento	Descrição e aplicação
Checklist de diagnóstico (CIS Controls IG1)	Instrumento de diagnóstico inicial para inventário de ativos, identificação de softwares não licenciados e mapeio de políticas de acesso.
Bitdefender GravityZone Business Security (255 licenças em nuvem)	Solução técnica para proteção de *endpoints* e registro de eventos de segurança, tendo como foco o monitoramento contínuo e suporte à intervenção.
GoPhish (hospedado em VPS na Oracle Cloud)	Ferramenta para criação e gestão de campanhas simuladas de *phishing* direcionadas a colaboradores selecionados, permitindo medir vulnerabilidade e resposta.

Diagnóstico inicial: Nessa fase, implementou-se o *checklist* baseado no IG1 para levantar a situação da infraestrutura e da governança de segurança. Foram identificados ativos de hardware, softwares instalados (incluindo usos não licenciados), práticas de uso de mídias removíveis e incidentes anteriores relevantes, como fraude bancária decorrente de comprometimento de estação da diretoria.

Intervenção técnica: Com base no diagnóstico, procedeu-se à instalação e configuração do Bitdefender GravityZone em 255 estações de trabalho, com ativação de módulos avançados de proteção, como controle de dispositivos e mecanismos de detecção de ameaças baseados em aprendizado de máquina. De modo paralelo, arquivos considerados críticos foram migrados de servidores locais vulneráveis para serviços em nuvem (Google Workspace e OneDrive), amenizando a dependência de infraestrutura física dispersa. Essa etapa trouxe relatórios consolidados de ameaças detectadas, uso de mídias removíveis e índice de conformidade com os controles do IG1.

Intervenção comportamental e validação: Previamente ao disparo das simulações, foi feita uma campanha de conscientização com disseminação de informativos internos, conforme detalhado na Seção 4.3. Na etapa final, foi conduzida uma campanha de phishing simulada utilizando o GoPhish. Para isso, adquiriu-se um domínio similar ao da organização (técnica de *typosquatting*), sobre o qual foi configurada uma página falsa de login do Google com certificado SSL/TLS válido. As mensagens foram disparadas via serviço de e-mail transacional com um gatilho de urgência (“redefinição de senha”), buscando reproduzir táticas comuns de engenharia social. Os indicadores coletados incluíram taxa de cliques nas iscas, envio de credenciais na *landing page* e número de usuários que reportaram o ataque como suspeito.

3.4. Procedimentos éticos

Considerando que a pesquisa envolve a participação de seres humanos e a coleta de dados em ambientes organizacionais virtuais, utilizou-se o Termo de Consentimento Livre e Esclarecido (TCLE). A aplicação do instrumento visou assegurar a transparência do estudo, garantindo que os participantes compreendessem plenamente os objetivos, riscos e benefícios envolvidos, o que confere maior confiabilidade e adequação normativa aos dados coletados.

Três salvaguardas éticas foram adotadas para a garantia da proteção dos participantes: (i) autorização institucional, o experimento foi respaldado pelo consentimento formal prévio da Diretoria; (ii) anonimização imediata, a ferramenta registrou de forma ex-

clusiva métricas comportamentais, sem capturar ou guardar senhas reais ou informações pessoais dos colaboradores; e (iii) abordagem pedagógica e não punitiva, os resultados foram tratados em nível agregado, sem identificação, exposição ou aplicação de sanções a nenhum participante, com finalidade unicamente diagnóstica e educativa. Esses procedimentos alinham-se aos princípios da LGPD [Brasil 2018] e às boas práticas de pesquisa em ambientes organizacionais.

4. Resultados

4.1. Diagnóstico do cenário anterior

O diagnóstico inicial confirmou um quadro de elevada exposição a riscos, que condiz com o perfil descrito na Seção 1: acesso direto à internet por provedores locais, sem VPN com a matriz e sem firewall de perímetro padronizado. O levantamento de ativos identificou uso disseminado de softwares não licenciados e ausência de inventário sistemático, o que dificultava a gestão de vulnerabilidades. Também foram registrados incidentes anteriores relevantes, incluindo o comprometimento de uma estação de diretoria que acabou resultando em fraude bancária não rastreável e a ocorrência de campanhas massivas de phishing que não eram filtradas de forma devida pelo serviço terceirizado de e-mail. Em conjunto, esses elementos caracterizavam um ambiente com baixa maturidade em segurança da informação e forte dependência de respostas não sistematizadas.

4.2. Intervenção técnica: neutralização de ameaças e aderência ao IG1

A implantação do Bitdefender GravityZone Business Security em 255 estações de trabalho permitiu, em primeiro lugar, obter visibilidade integrada sobre o parque de *endpoints* distribuídos. A partir da geração dos relatórios, foi possível quantificar a extensão das ameaças previamente ativas na infraestrutura.

Na Figura 1, é evidenciado um relatório com um ranking dos malwares mais detectados.

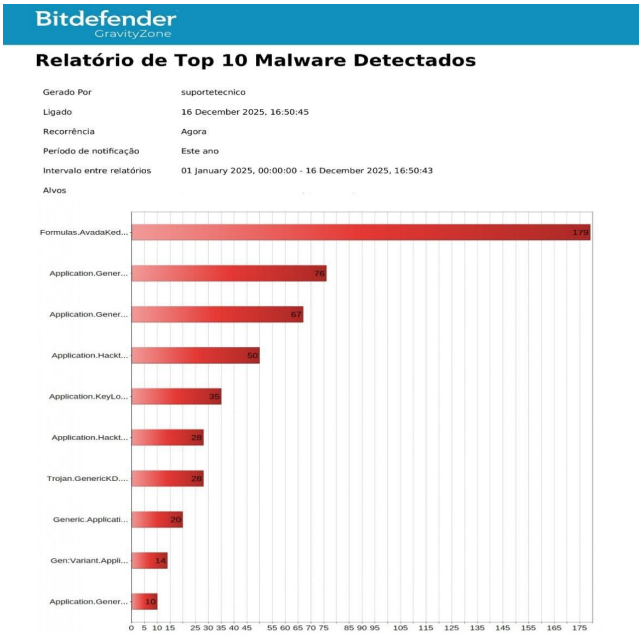

Figura 1. Relatório das *top* 10 ameaças detectadas e neutralizadas pelo Bitdefender GravityZone.

No período analisado, mais de 500 ameaças foram detectadas e neutralizadas, incluindo 35 instâncias de *spywares* e *keyloggers*, associados diretamente ao risco de exfiltração de credenciais e dados sensíveis, e 179 scripts maliciosos e *hacktools*, em grande parte interligados à ativação ilegal de softwares. Em paralelo, o módulo de controle de dispositivos registrou mais de 350 conexões USB em um único mês, evidenciando uma cultura de uso massivo de mídias removíveis ausente de controles prévios.

A partir da configuração dos módulos avançados de proteção e da aplicação das salvaguardas previstas no IG1, o relatório de conformidade do fabricante evidenciou índice global de 82% de aderência às práticas de higiene cibernética essenciais. As pendências remanescentes foram mapeadas para ciclos posteriores, de modo a não comprometer a usabilidade dos sistemas e a rotina administrativa.

Do ponto de vista econômico, o investimento em licenças, calculado para cinco anos de uso, resultou em custo aproximado de R$ 26,21 por usuário ao ano, considerado compatível com as restrições orçamentárias da organização. Esses números reforçam a viabilidade do IG1 como estratégia de elevação de maturidade em ambientes de recursos limitados.

4.3. Intervenção comportamental: suscetibilidade a phishing

Previamente ao disparo das simulações, a organização gerenciou uma campanha de conscientização com a disseminação de informativos internos sobre segurança da informação, buscando sensibilizar os colaboradores para práticas básicas de higiene digital — entre elas, a checagem de remetentes e a desconfiança diante de mensagens com gatilhos de urgência. Apenas após essa etapa de preparação foi realizada a avaliação prática da suscetibilidade humana.

Na etapa de avaliação do fator humano, foram disparadas 137 mensagens de phishing simuladas para colaboradores selecionados, usando domínio com *typosquatting* e página falsa de login do Google hospedada na VPS alterada para o experimento. O conteúdo dos e-mails explorava um gatilho de urgência relacionado à redefinição de senha, buscando reproduzir táticas recorrentes de engenharia social.

Os registros do GoPhish apontaram taxa de 34% de interação inicial: aproximadamente um em cada três destinatários clicou no link presente na mensagem fraudulenta. Mais grave, 15% dos usuários (21 pessoas) inseriram suas credenciais corporativas na *landing page* falsa, o que, em um cenário real, possibilitaria tomada de contas, movimentação lateral na rede e eventual propagação de *ransomware* ou outras formas de ataque.

Por outro lado, 25 participantes reportaram o e-mail como suspeito aos canais internos, o que levou a plataforma Google Workspace a bloquear automaticamente o domínio malicioso para toda a organização após as primeiras denúncias. Esse comportamento mostra a presença de um núcleo de colaboradores com maior percepção de risco, capaz de atuar como sensor de ameaças em uma estratégia de defesa colaborativa.

É importante ressaltar que os grupos não são mutuamente exclusivos: parte dos colaboradores que reportaram o e-mail pode ter interagido com o link antes de identificá-lo como suspeito.

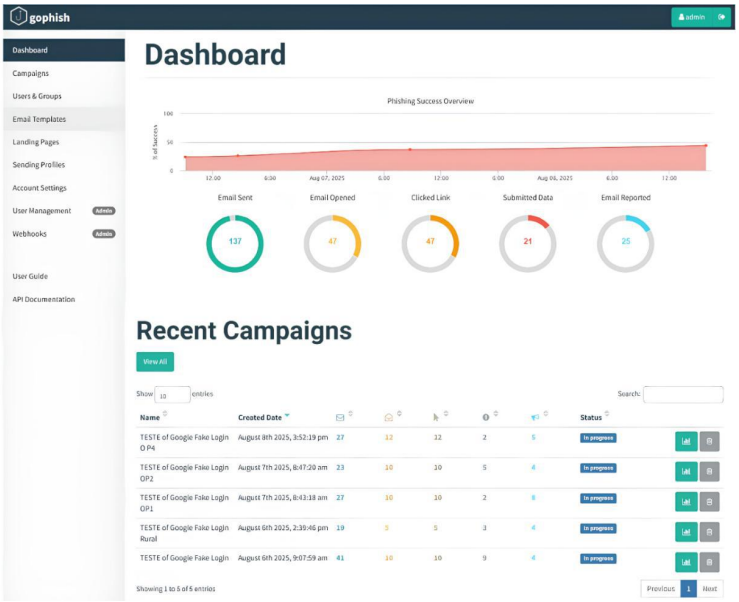

Figura 2. Resultados da campanha de *phishing* simulada via GoPhish.

4.4. Síntese comparativa dos indicadores de maturidade

Os resultados permitem a sintetização, em quatro dimensões, a transformação obtida com a aplicação do IG1 — gestão de ativos, proteção de *endpoint*, controle de mídias removíveis e fator humano —, com cada dimensão mapeada ao respectivo controle do *framework* que a fundamenta. A Tabela 2 consolida os principais indicadores coletados antes e após a intervenção.

Tabela 2 - Síntese comparativa antes e após a implementação do CIS Controls IG1, com mapeamento dos controles aplicados.

Dimensão	**Controle CIS**	**Antes da intervenção**	**Após a intervenção**
Gestão de ativos e inventário	CIS 1 & 2	Sem inventário sistemático; softwares não licenciados disseminados	Levantamento completo de ativos; softwares mapeados e irregularidades identificadas
Proteção de *endpoint*	CIS 10	Inexistente ou dispersa; sem monitoramento consolidado	255 estações protegidas pelo Bitdefender GravityZone
Ameaças ativas	CIS 10	Desconhecidas; sem registro ou monitoramento	Mais de 500 neutralizadas (35 *spywares/keyloggers*; 179 scripts maliciosos)
Controle de mídias removíveis	CIS 3	Sem política ou registro de uso	Mais de 350 conexões USB monitoradas em um único mês
Aderência ao IG1	CIS 1–18	Não avaliada; processos *ad hoc*	82% de conformidade com as práticas essenciais
Custo por usuário/ano	CIS 10	Não mensurado	R$ 26,21 (projeção para 5 anos de uso)
Suscetibilidade a phishing	CIS 14	Desconhecida; sem simulações ou treinamentos	34% de cliques; 15% forneceram credenciais; 25 reportaram proativamente

No conjunto, os achados mostram que a adoção do CIS Controls IG1 permitiu à organização migrar de uma postura *ad hoc*, baseada em respostas pontuais a inciden-

tes, para um modelo de gestão técnica sistematizada, com métricas auditáveis nas quatro dimensões mapeadas e alinhamento mais consistente às exigências da LGPD.

5. Discussão: implicações sociais, jurídicas e organizacionais

Os resultados obtidos evidenciam que as fragilidades identificadas na organização não se limitavam a questões internas de TI, mas tinham potencial para afetar de forma direta a proteção de dados pessoais, a continuidade de serviços e a confiança de parceiros e usuários. Do ponto de vista jurídico, o cenário inicial descrito no diagnóstico — com malwares persistentes, keyloggers, uso intensivo de mídias removíveis sem controles e histórico de fraude bancária — configurava alto risco em relação ao dever de segurança previsto no Artigo 46 da LGPD [Brasil 2018]. A implantação de controles de *endpoint* alinhados ao CIS Controls IG1 cooperou para materializar esse dever, ao bloquear ameaças ativas, reduzir a superfície de ataque e produzir evidências documentais de salvaguardas técnicas adotadas. Esse movimento, também, eleva a força da capacidade de demonstrar *accountability*, conforme enfatiza o Artigo 50, ao interligar práticas concretas de proteção às políticas jurídicas em processo de formalização.

Organizacionalmente, a transição de um modelo corretivo e não estruturado, baseado em respostas a incidentes pontuais, para uma gestão técnica estruturada de segurança demonstra avanço em maturidade. O índice de 82% de aderência às práticas de higiene do IG1 mostra que, mesmo em ambientes com restrição orçamentária, é possível estruturar controles mínimos com impacto mensurável, desde que priorizados de forma realista. O custo anual de aproximadamente R$ 26,21 por usuário aprimora a viabilidade dessa estratégia para PMEs e entidades similares, sugerindo que a ausência de segurança nem sempre decorre apenas de limitações monetárias, mas também de ausência de planejamento e de processos formais [Duarte and Rizo 2024].

A dimensão humana dos resultados traz elementos críticos para o debate em Computação e Sociedade. A taxa de 34% de cliques e 15% de envio de credenciais nas simulações de phishing confirma que uma parcela significativa dos colaboradores permanece vulnerável a técnicas básicas de engenharia social [Mitnick and Simon 2003, Kanagusku and Gaseta 2023]. Em um contexto regido pela LGPD, essa suscetibilidade não é apenas um problema operacional: ela representa risco concreto à confidencialidade e integridade de dados pessoais, incluindo informações sensíveis tratadas pela organização. Ao mesmo tempo, o fato de 25 usuários terem reportado de forma proativa as mensagens suspeitas evidencia que programas de conscientização têm potencial para criar uma "defesa colaborativa", na qual colaboradores atuam como sensores de ameaças que alimentam os mecanismos automatizados de proteção.

Sob a perspectiva social, a experiência analisada ilustra como assimetrias de proteção entre grandes corporações e organizações de menor porte podem ser parcialmente mitigadas por frameworks práticos como o CIS Controls, desde que adaptados à realidade local. Em regiões como a Amazônia Legal, onde OSCIPs e PMEs possuem um papel relevante na execução de políticas e projetos, falhas de segurança podem amplificar desigualdades já existentes, afetando justamente populações que dependem dos serviços prestados. Ao fortalecer a infraestrutura de segurança e estabelecer métricas de maturidade, a organização reduz a probabilidade de interrupções e incidentes que poderiam acabar comprometendo dados e serviços de grupos vulneráveis.

Como síntese orientadora para organizações em contexto similar, destacam-se três diretrizes práticas compatíveis com restrições financeiras e operacionais: (i) dar prioridade a proteção de *endpoints* com acesso direto a dados críticos antes de qualquer outro controle; (ii) adotar soluções em nuvem com licenciamento por usuário para viabilizar escala sem investimento em infraestrutura física; e (iii) incluir simulações periódicas de *phishing* como métrica contínua de maturidade humana, articuladas a campanhas de conscientização anteriores ao disparo.

6. Considerações Finais

Este estudo demonstrou que a adoção estruturada do CIS Controls v8 IG1 é uma estratégia viável e eficaz para elevar a maturidade de cibersegurança em organizações com recursos limitados, respondendo diretamente à questão norteadora da pesquisa e evidenciando que assimetrias de proteção cibernética entre organizações de grande e pequeno porte podem ser parcialmente mitigadas por frameworks acessíveis, o que é especialmente relevante em regiões como a Amazônia Legal, onde OSCIPs e PMEs possuem um papel de importância na execução de serviços públicos e sociais. Mais do que confirmar a aplicabilidade técnica do framework, os resultados indicam que a principal barreira à segurança nesse perfil institucional não é necessariamente financeira, mas decorre da falta de processos de formalização e de uma postura organizacional proativa [Duarte and Rizo 2024].

A intervenção produziu resultados mensuráveis em três frentes: técnica, econômica e humana. Na dimensão técnica, houve neutralização de mais de 500 ameaças ativas e atingido 82% de aderência ao IG1, com geração de evidências documentárias de salvaguardas alinhadas aos Artigos 46 e 50 da LGPD [Brasil 2018]. Na dimensão econômica, o custo de R$ 26,21 por usuário ao ano reforça a viabilidade do modelo para organizações com orçamento restrito. Na dimensão humana, a taxa de 34% de interação em simulações de *phishing*, feitas após campanha prévia de conscientização, evidencia que desafios de literacia digital persistem mesmo após intervenções educativas, reforçando a necessidade de programas contínuos [Kanagusku and Gaseta 2023].

Por tratar-se de um Estudo de Caso [Yin 2015], os achados permitem generalização analítica, isto é, a extrapolação para proposições teóricas sobre implementação de controles em organizações com recursos limitados, mas não generalização estatística. Três limitações específicas precisam ser reconhecidas: (i) o índice de 82% de aderência foi obtido a partir de relatório gerado pela própria solução de *endpoint*, o que pode introduzir viés de mensuração; (ii) a amostra da campanha de *phishing* (137 colaboradores) representa apenas parte dos usuários da organização; e (iii) o recorte temporal único impede afirmações sobre a sustentabilidade dos controles a longo prazo.

Como trabalhos futuros, destacam-se: (i) replicar o estudo em outras OSCIPs e PMEs de setores distintos para comparações interinstitucionais; (ii) focar na dimensão qualitativa com entrevistas e grupos focais sobre percepções de risco e literacia digital; e (iii) integrar *endpoints* a mecanismos de detecção e correlação de logs para monitoramento contínuo.

Referências

Barracuda Networks (2022). Spear phishing: Top threats and trends. Disponível em: https://www.barracuda.com/company/news/2022/845. Acesso em: 02 nov. 2024.

Brasil (2018). Lei nº 13.709, de 14 de agosto de 2018. dispõe sobre a proteção de dados pessoais e altera a lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 03 jan. 2026.

Center for Internet Security (2021). CIS Controls v8. Disponível em: https://www.cisecurity.org/controls. Acesso em: 02 nov. 2024.

CERT.br (2020). Cartilha de segurança para internet: Fascículo trabalho remoto. São Paulo: Comitê Gestor da Internet no Brasil. Disponível em: https://cartilha.cert.br/fasciculos/trabalho-remoto/fasciculo-trabalho-remoto.pdf. Acesso em: 15 out. 2025.

Deloitte (2021). Estratégias para um futuro cibernético: pesquisa global de segurança cibernética. Disponível em: https://www.deloitte.com/br/pt/about/press-room/release-estrategias-futuro-cibernetico.html. Acesso em: 15 dez. 2025.

Duarte, C. M. d. C. and Rizo, A. C. (2024). Segurança da informação no contexto empresarial: uma análise das lacunas na aplicação de políticas e treinamentos. In *FatecSeg – Congresso de Segurança da Informação*, volume 1, [S. l.]. Acesso em: 24 jan. 2026.

Federação do Comércio do Estado de São Paulo (2024). Pequenas e médias empresas são o alvo da maioria dos ataques cibernéticos. Disponível em: https://www.fecomercio.com.br/noticia/pequenas-e-medias-empresas-sao-o-alvo-da-maioria-dos-ataques-ciberneticos. Acesso em: 03 nov. 2024.

Fontes, E. and Truzzi, G. (2020). Cartilha trabalho remoto: Recomendações para a garantia da segurança jurídica e da informação. E-book.

Kanagusku, A. R. A. and Gaseta, E. (2023). Fator humano na segurança da informação: desmistificando o elo mais fraco. In *FatecSeg – Congresso de Segurança da Informação*, [S. l.]. Acesso em: 25 jan. 2026.

Kaspersky (2023). PMEs recebem 365 tentativas de ataque por minuto no Brasil, veja como se proteger. Kaspersky Brasil, 4 dez. 2023. Disponível em: https://www.kaspersky.com.br/about/press-releases/kaspersky-pmes-recebem-365-tentativas-de-ataque-por-minuto-no-brasil-veja-como-se-proteger. Acesso em: 18 nov. 2024.

Machado, F. N. R. (2014). *Segurança da informação: princípios e controle de ameaças*. Érica, São Paulo.

Menchão, C. T. d. S., Almeida, M. S. d., and Glória Junior, I. (2024). Estudo de caso sobre a importância do plano de continuidade de negócios após um ataque de Ransomware. In *FatecSeg – Congresso de Segurança da Informação*, volume 1, [S. l.]. Acesso em: 24 jan. 2026.

Mitnick, K. D. and Simon, W. L. (2003). *A arte de enganar: ataques de hackers: controlando o fator humano na segurança da informação*. Pearson Makron Books, São Paulo.

Nakamura, E. T. and Geus, P. L. (2007). *Segurança de redes em ambientes cooperativos*. Novatec Editora, São Paulo.

Segal, E. (2022). Small businesses are more frequent targets of cyberattacks than larger companies: New report. Forbes. Disponível em: https://www.forbes.com/sites/edwardsegal/2022/03/30/cyber-criminals/. Acesso em: 17 nov. 2024.

Stallings, W. and Brown, L. (2014). *Segurança de computadores: princípios e práticas*. Elsevier, Rio de Janeiro, 2 edition.

Thiollent, M. (2011). *Metodologia da pesquisa-ação*. Cortez, São Paulo, 18 edition.

Verizon Business (2025). 2025 Data Breach Investigations Report (DBIR). Disponível em: https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf. Acesso em: 14 fev. 2026.

Yin, R. K. (2015). *Estudo de caso: planejamento e métodos*. Bookman, Porto Alegre, 5 edition. Tradução de Cristhian Matheus.