Conscientização em Segurança da Informação no Serviço Público, um modelo para implementação no Ministério da Fazenda e demais órgãos da Administração Pública Federal

Rafael Mendes Marques de Brito
Universidade de Brasília (UnB)
Brasília, DF, Brasil

Prof. Dr. Luiz Antonio Ribeiro Junior
Universidade de Brasília (UnB)
Brasília, DF, Brasil

***Resumo*—A segurança da informação no setor público brasileiro é vulnerável primariamente não a ataques técnicos sofisticados, mas a vulnerabilidades comportamentais. Incidentes relacionados a erro humano constituem 85-95% do total de incidentes em organizações públicas e privadas. Este trabalho propõe modelo integrado de conscientização em segurança da informação estruturado em três dimensões complementares: priorização baseada em evidências científicas, pedagogia fundamentada em andragogia e reforço espaçado, e operacionalização pragmática através de governança formal, ferramenta tecnológica centralizada e mensuração contínua. Através de revisão sistemática de literatura, análise de frameworks internacionais e arcabouço normativo brasileiro, o trabalho identifica que conscientização é requisito mandatório de conformidade, não recomendação opcional. Aplicação de princípios pedagógicos comprovados (microlearning combinado com gamificação e reforço espaçado) produz retenção e mudança comportamental substantivamente superior. O modelo proposto operacionaliza conscientização através de: programa permanente institucionalizado em normativos; ferramenta centralizada de entrega e mensuração; conteúdo multimodal segmentado por público; reconhecimento pragmático de dilemas reais entre segurança ideal e produtividade operacional; mensuração em três camadas (processo, comportamento, impacto); e engajamento de liderança executiva. Implementação faseada em piloto no Ministério da Fazenda com posterior expansão para órgãos congêneres oferece caminho concreto para transformação de realidade de segurança da informação no setor público brasileiro, reduzindo vulnerabilidades causadas por erro humano e criando cultura organizacional na qual segurança é responsabilidade compartilhada e contínua.**

***Index Terms*—Conscientização em Segurança da Informação; Fator Humano; Segurança no Setor Público; Pedagogia de Segurança; Microlearning; Gameficação; Governança de SI; Administração Pública Federal.**

1. INTRODUÇÃO E CONTEXTUALIZAÇÃO

1.1 Visão Crítica da Segurança na Administração Pública Federal

A Administração Pública Federal (APF) no Brasil enfrenta problemas crescentes em segurança da informação. A mudança digital rápida, acelerada pela pandemia COVID-19, aumentou a superfície de ataque por meio do trabalho remoto, sistemas conectados e uso de plataformas em nuvem. Ao mesmo tempo, ameaças cibernéticas evoluem em sofisticação: ransomware direcionado a órgãos públicos, phishing específico ao contexto governamental e exploração de vulnerabilidades zero-day.

A APF é depositária de informações pessoais sensíveis para o país. Essas informações incluem por exemplo dados de impostos, segurança social e defesa. Comprometer essas informações não afeta apenas a organização, mas também a confiança pública em instituições governamentais. Quando sistemas críticos são interrompidos, há impacto direto na prestação de serviços aos cidadãos [1].

1.2 Incidentes Críticos: O Caso SIAFI e Operação Gold Digger

Em 2024, a operação *Gold Digger* afetou o Sistema Integrado de Administração Financeira (SIAFI) — um sistema crítico que gerencia todas as transações financeiras do governo federal. O ataque não ocorreu por causa de uma falha técnica sofisticada, mas pela exploração de vulnerabilidades ligadas ao fator humano: senhas comprometidas através de campanhas de phishing, acesso não autorizado utilizando credenciais de gestores e ordenadores de despesas e emissão fraudulenta de certificados digitais [2].

Esse evento estabeleceu um precedente importante: a segurança da APF não é exclusivamente um problema técnico que infraestrutura moderna soluciona. É um problema que envolve comportamento humano, processos organizacionais e cultura institucional.

1.3 O Fator Humano como Ponto Fraco Principal

Estudos demonstram que o fator humano é crucial para ataques cibernéticos bem-sucedidos. Não é meramente um "elo fraco"genérico. É uma vulnerabilidade real, observável, previsível e redutível através de conscientização efetiva [1], [3].

Atos como compartilhamento de credenciais, cliques em links maliciosos, acesso a sites comprometidos, instalação de software não autorizado e desatenção com computadores desbloqueados representam os meios pelos quais atacantes obtêm acesso [1]. Esses atos não refletem falta de honestidade dos servidores públicos. Evidenciam lacunas no conhecimento,

pressões conflitantes do trabalho e contextos nos quais segurança não é priorizada [3].

1.4 Estrutura Legal e Normativa

Várias leis e regulamentos estabelecem regras e diretrizes para a segurança da informação na Administração Pública Federal:

- **Política Nacional de Segurança da Informação (PNSI):** Define diretrizes estratégicas para segurança de informações em órgãos federais [4].
- **Lei Geral de Proteção de Dados (LGPD):** Cria obrigação de proteção de dados pessoais [5].
- **Estratégia Nacional de Cibersegurança (E-Ciber):** Objetivo de elevar a segurança e a resiliência cibernéticas nacionais, aproximando-se da realidade dos países mais avançados na temática [6].

Esses marcos regulatórios indicam que proteção adequada requer abordagem integrada que combine tecnologia, processos e recursos humanos. Conscientização é mencionada explicitamente em muitos documentos como componente essencial.

1.5 Vulnerabilidades do Fator Humano: Dimensão do Problema

A segurança da informação frequentemente é tratada como problema exclusivamente técnico. Análise mais aprofundada revela que fragilidades em comportamentos são elemento crítico frequentemente negligenciado. Levantamento sistemático identificou 97 ações de risco não intencionais de usuários de ambientes virtuais, distribuídas em dez categorias principais: Autenticação e Senhas, Privacidade de Dados, Segurança de Dispositivos, Uso de E-mail, Uso da Internet, Acesso Físico, Política de Mesa Limpa, Segurança Móvel e Conformidade com Políticas [1].

Esses comportamentos não refletem desonestidade ou incompetência. Refletem falta de conhecimento, pressões de trabalho conflitantes ou ambientes nos quais segurança não é adequadamente valorizada. Dados empíricos ilustram a magnitude: 63% mantêm senhas anotadas no local de trabalho [7]; 78% não modificam senhas com frequência recomendada [8]; 50% dos computadores em ambientes hospitalares permanecem desbloqueados durante períodos de inatividade [9]; e 84% de usuários instalam software ilegal [10].

Evidências internacionais demonstram impacto significativo: O Relatório Verizon Data Breach Investigations Report (DBIR) de 2023 indicou que 74% de todas as violações de dados envolvem fator humano [1]. O Fórum Econômico Mundial estimou que 95% dos problemas de segurança resultam de falhas humanas [1]. No setor público, essas vulnerabilidades são agravadas por condições específicas: conflito entre mandatos de trabalho (tarefas urgentes) e segurança (proteção preventiva), infraestrutura técnica inadequada, políticas de segurança sem aplicação efetiva e estruturas hierárquicas que dificultam denúncia de problemas [3].

Importante notar que revisão cuidadosa examinando dez estudos originários de múltiplos países (Arábia Saudita, Polônia, Romênia, Inglaterra, Brasil, Croácia) com populações distintas revelou que a universalidade dos desafios de segurança comportamental é consistente; vulnerabilidades semelhantes aparecem em todos os contextos estudados [1]. Este não é problema localizado, mas fenômeno generalizado.

1.6 Justificativa e Lacuna a Ser Preenchida

Lacuna Identificada: O Ministério da Fazenda, como órgão solicitante dos serviços administrativos prestados pelo ColaboraGov [11], enfrenta restrições significativas na implementação de controles técnicos de infraestrutura. Sua participação no modelo centralizado de compartilhamento de serviços de suporte administrativo limita a autonomia sobre decisões de segurança em nível de infraestrutura, que são coordenadas de forma centralizada pelo Ministério da Gestão e da Inovação em Serviços Públicos (MGI).

Diante dessa restrição estrutural, a organização identifica uma oportunidade estratégica: focar em variável que permanece sob seu controle direto e que é de elevada importância para a segurança geral — o comportamento de seus servidores e usuários. Diferentemente de controles técnicos que dependem de decisões compartilhadas em âmbito federal, a conscientização em segurança da informação dos colaboradores é responsabilidade exclusiva do órgão. É nesse contexto que se torna crítico implementar estrutura comprovadamente efetiva de conscientização em segurança que aborde vulnerabilidades do fator humano de forma sistemática, contínua e pedagogicamente validada. .

Propósito deste Trabalho: Elaborar um modelo de programa de conscientização em segurança da informação adaptado ao contexto específico do Ministério da Fazenda e da infraestrutura compartilhada ColaboraGov, fundamentado em: (1) melhores práticas internacionais (ISO, NIST, COBIT), (2) metodologias pedagógicas com efetividade comprovada (microlearning, gamificação, simulações), (3) compreensão das condições específicas do setor público (pressões operacionais, hierarquia, restrições orçamentárias).

—

2. A IMPORTÂNCIA RELATIVA DA CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO

2.1 O Fator Humano como Elemento Determinante

Segurança da informação é frequentemente abordada sob ótica exclusivamente técnica: firewalls, antivírus, criptografia, controle de acesso. Estas meidadas técnicas são necessárias, porém, não são suficientes para garantir uma efetiva segurança da informação. Tecnologia protege sistemas e pessoas protegem dados. Quando uma pessoa compromete o acesso (compartilhando senha, clicando em phishing), mesmo com o melhor firewall existente não prevenirá a violação.

Pesquisa sistemática estabeleceu que fator humano é elemento determinante em violações. Não é “elo fraco”. É componente central da postura de segurança organizacional. Ignorar fator humano é como construir castelo com alicerces

frágeis: estrutura superior pode ser impressionante, mas colapsa sob pressão [12].

2.2 Consciência versus Conformidade: Distinção Crítica

A distinção entre conformidade e consciência no ambiente organizacional está amplamente discutida na literatura de segurança da informação. Conforme Albrechtsen & Hovden (2010) [13], a conformidade diz respeito ao cumprimento de normas e procedimentos devido à imposição ou controle externo, frequentemente sem uma compreensão real dos riscos: isso pode levar a atitudes automáticas ou superficiais, como a escolha de senhas previsíveis apenas para atender a requisitos formais. Por outro lado, consciência em segurança refere-se a um entendimento genuíno dos riscos e impactos, resultando em escolhas pró-ativas e sustentáveis, mesmo na ausência de fiscalização direta [13], [14]. Estudos recentes apontam que políticas baseadas apenas em exigências normativas tendem a gerar resultados frágeis, enquanto iniciativas focadas na compreensão contextualizada dos riscos são mais eficazes para estimular comportamentos seguros e duradouros [14].

Um exemplo mais tangível no contexto público: funcionário que recebe mensagem "Não clique links desconhecidos" (conformidade) pode continuar clicando quando sob pressão de trabalho ("preciso responder este e-mail rapidamente"). Funcionário que compreende "Links phishing roubam credenciais, comprometendo segurança da instituição" (consciência) está mais propenso a validar origem mesmo sob pressão. A diferença é o conhecimento contextualizado.

2.3 Papel de Conscientização na Construção de Cultura Organizacional de Segurança

Cultura organizacional de segurança é onde segurança não é visto como "imposição do TI" ou "conformidade regulatória", mas como valor compartilhado. Nesta cultura:

- Servidores reconhecem que segurança é responsabilidade coletiva
- Reportar incidente é visto como ato correto, não admissão de falha pessoal
- Liderança demonstra pessoalmente compromisso com segurança
- Desvios são corrigidos com educação, não punição
- Segurança é conversação contínua, não treinamento anual isolado

Conscientização efetiva é catalisador que move organização de conformidade para cultura. Não acontece espontaneamente. Requer investimento intencional em educação contínua, comunicação clara, liderança visível [15], [16] [17].

2.4 Impacto Quantificável de Conscientização: Evidência Empírica

Além de argumentação teórica, há evidência empírica de impacto de conscientização. Estudos demonstram que programas de conscientização bem estruturados produzem resultados mensuráveis em redução de incidentes relacionados a fator humano [12]. Usuários conscientes identificam e reportam incidentes mais rapidamente [18], reduzindo "tempo de permanência" do atacante. Conformidade com políticas aumenta de forma significativa em organizações com programas de conscientização implementados [12], [18]. Os custos de violações de dados são substanciais — estimados entre 3 a 6 trilhões de dólares anuais globalmente [12] — tornando conscientização preventiva um investimento economicamente racional.

2.5 Consciência em Contextos Públicos: Diferenças Cross-Culturais e Setoriais

Pesquisa específica em organizações públicas revelou particularidades significativas entre diferentes contextos nacionais [19]:

- **Contexto Sueco**: Cultura de confiança e responsabilidade compartilhada facilita conscientização
- **Contexto Francês**: Hierarquia e estrutura formal requerem comunicação de segurança através de canais oficiais
- **Contexto Tunisiano**: Hierarquia rígida cria hesitação em reportar incidentes por medo de punição

Implicação para Administração Pública Federal: abordagem de conscientização deve ser sensível a contexto hierárquico da administração pública brasileira, criando espaço psicológico seguro para reporte e aprendizado, não punição.

2.6 Redução de Vulnerabilidades através de Conscientização Efetiva

Vulnerabilidades do fator humano não são inevitáveis nem imutáveis. Dados documentam que consciência efetiva reduz risco de forma quantificável.

1) Retenção de Conhecimento através de Reforço Contínuo

Pesquisa sistemática sobre escalas de consciência em segurança da informação identificou que reforço contínuo é crítico para manutenção de conhecimento [12].Programas que implementam reforço contínuo mantêm retenção significativamente superior comparado a treinamento único. Isto é crítico porque, conforme teorizado por Ebbinghaus (1885) [20], vulnerabilidades comportamentais reaparecem rapidamente sem reforço. Taherdoost [18] documentou que "cybersecurity awareness produces immediate, specific, and short-term learning unless the exercises are performed repeatedly". Microlearning implementa o spacing effect de Ebbinghaus, entregando conteúdo em pequenas doses ao longo do tempo, mantendo aprendizado e retenção ativo continuamente [18], [21].

2) Redução de Comportamentos de Risco Específicos

Modelos inovadores de conscientização em segurança cibernética integram componentes de gamificação, jogos sérios e microlearning que demonstram efetividade em redução de comportamentos de risco [18]. Estudos documentam que programas gamificados produzem aumento de 51,4% em consciência de trabalhadores sobre cibersegurança, com 79% dos participantes aprendendo informação nova e 84% dos participantes engajados [18].

3) Conformidade Organizacional através de Engajamento de Liderança

Programas com engajamento explícito de liderança apresentam melhor taxa de conformidade comparado a programas

sem suporte de liderança [12]. Isto sugere que conscientização não funciona isoladamente, mas é multiplicada por sinais organizacionais claros.

Implicação: Se diretor de departamento regularmente muda sua senha, bloqueia computador, valida e-mails antes de compartilhar, mensagem silenciosa mas poderosa é enviada a subordinados: "segurança é importante aqui".

4) Exemplos Documentados em Setor Público Brasileiro

Estudo ergonômico em instituição pública federal brasileira documentou comportamentos inseguros de funcionários identificados através de observação direta e análise de incidentes reportados [3]. Especificamente:

- Compartilhamento de senhas: 7 casos documentados
- Não bloqueio de estações de trabalho ao se ausentar: 6 casos
- Violação de política de mesa limpa: 6 casos
- Armazenamento inadequado de dados corporativos em mídias removíveis
- Utilização de equipamentos pessoais na rede institucional

Estes comportamentos, quando se adotou abordagem ergonômica para análise, revelaram que as dificuldades em seguir as recomendações de segurança estão frequentemente relacionadas a conflitos na própria organização do trabalho, não apenas a falta de conformidade [3].

3. ABORDAGENS PEDAGÓGICAS E MODELOS DE APRENDIZADO

3.1 Fundamentos Pedagógicos Aplicados à Educação em Segurança da Informação

Educação em segurança da informação baseia-se em fundamentos pedagógicos consolidados. Adultos aprendem melhor quando conteúdo é prático, relevante e conectado a experiências prévias [22]. Conhecimento é construído através de experiência e reflexão, não apenas transmissão passiva [23]. Comportamentos são reforçados quando reconhecidos positivamente [18].

Para retenção de conhecimento em segurança, crítico movimentar informação de retenção de curto para longo prazo através de reforço e prática repetida [24].

1) Curva do Esquecimento e Implicações para Reforço

Ebbinghaus [20] demonstrou que retenção de informação decai dramaticamente sem reforço. Sem revisão, pessoas esquecem aproximadamente 50% da informação aprendida após uma hora, 70% após 24 horas, e 90% após uma semana [24].

O espaçamento de revisões em intervalos estratégicos (imediatamente após aprendizado, após 1 dia, após 3 dias, após 1 semana, após 1 mês) pode manter retenção acima de 90%. Pesquisa sistemática de retenção de conhecimento mostrou que reforço contínuo mantém retenção significativamente superior após períodos prolongados, comparado a treinamento único, destacando que reforço mensal é essencial para manutenção de conhecimento [12].

Esta descoberta tem implicação direta para conscientização em segurança: uma sessão única de treinamento não mantém conhecimento. Revisão contínua é essencial. Conforme demonstrado em Seção 3, programa efetivo requer reforço contínuo de mensagens sobre segurança.

3.2 Microlearning: Aprendizado em Pequenos Passos

Microlearning é abordagem pedagógica que entrega conteúdo em pequenas unidades, focadas, auto-contidas, tipicamente com duração de 5-15 minutos. Tornou-se especialmente popular desde 2005 [24] e ganhou momentum significativo durante pandemia COVID-19.

1) Definição e Características Fundamentais

Microlearning caracteriza-se por conteúdo bite-sized, autocontido, focado topicamente, interativo, com feedback imediato e acessível via mobile [21]. Conforme demonstrado em revisão sistemática, características principais incluem:

- Pequeno o suficiente para ser consumido em período breve sem carga cognitiva excessiva
- Compreensível sem necessidade de informação externa adicional
- Aborda um conceito ou objetivo de aprendizado específico
- Permite participação do aprendiz, não apenas consumo passivo
- Fornece resposta instantânea sobre desempenho
- Disponível em dispositivos portáteis, acessível qualquer hora [24]

2) Vantagens Empíricas Comprovadas

Pesquisa sistemática identificou vantagens substantivas de microlearning:

- **Retenção superior**: Estudos sistemáticos mostraram que microlearning produz retenção superior em relação a treinamentos longos únicos [21]
- **Maior engajamento**: Estudos mostraram engajamento superior em conteúdo microlearning em comparação a videoaulas tradicionais [24]
- **Maior motivação**: Participantes relatam maior motivação em microaprendizado, particularmente quando integrado a trabalho prático [24]
- **Flexibilidade**: Acesso assincrônico permite aprendizado no momento e local que melhor se adequa ao aprendiz
- **Redução de ansiedade**: Estudos mostraram que microlearning com gamificação reduz ansiedade significativamente [25]. Estudos especializados encontraram que microlearning produz maior retenção de conhecimento, auto-eficácia aumentada, maior engajamento e motivação [21]

3) Limitações e Quando Não Usar

Não obstante vantagens, microlearning tem limitações importantes [21], [24]:

- **Insuficiente para conhecimento profundo**: Quando objetivo é compreensão profunda de tópico complexo, microlearning isolado pode ser inadequado. Necessita integração com aprendizados mais profundos
- **Risco de conhecimento fragmentado**: Microunidades isoladas podem criar percepção de conhecimento desconectado. Requer vinculação clara a conceitos maiores

- **Inadequado como aprendizado único**: Microlearning é mais efetivo como reforço que como estratégia única de aprendizado
- **Design complexo**: Contrário à aparência de "pequeno", desenho efetivo de microconteúdo é pedagogicamente complexo e requer cuidado de design
- **Falta de contexto inicial**: Aprendiz novo em tópico pode não ter contexto suficiente para compreender microcápsula sem introdução maior
- **Ambiente distraído**: Microlearning assume ambiente com atenção disponível. Em ambiente ruidoso ou com distrações, pode ser inefetivo

Pesquisa sistemática mostra que microlearning é mais efetivo quando: (1) complementa aprendizado mais profundo, (2) reforça conhecimento já existente, (3) aborda tópico circunscrito, (4) entrega em ambiente onde aplicação prática é possível [21].

4) Implementação Prática: Princípios de Design

Revisão sistemática identificou princípios criticamente importantes para design de microlearning efetivo [24]:

Design de Conteúdo Microlearning:

- Dividir em unidades pequenas, bite-sized, focadas (5-15 minutos)
- Usar linguagem clara, concisa, sem jargão desnecessário
- Estruturar com objetivo de aprendizado claro (o que aprendiz será capaz de fazer)
- Usar múltiplos formatos de mídia: vídeo curto (mais popular), texto estático, infográficos, quizzes
- Conteúdo deve ser relevante e prático, conectado a contexto do aprendiz
- Usar cores estratégicas e ícones para melhorar reconhecimento

Fluxo Instrucional de Microaprendizado:

- Descrever objetivo de aprendizado claramente
- Usar diferentes e atraentes formatos de mídia
- Encorajar interação (not passive consumption)
- Incluir práticas e tarefas hands-on
- Fornecer feedback imediato durante ou logo após
- Permitir auto-avaliação
- Conectar a conhecimento prévio do aprendiz

Estudos em contextos variados demonstraram que tamanho ideal varia por conteúdo: durações de 5-10 minutos foram mais populares que conteúdo muito breve [21].

3.3 Gamificação em Treinamento de Segurança

Gamificação refere-se à aplicação de elementos de design de jogos (pontos, badges, leaderboards, progresso visual, narrativa) em contextos não-lúdicos como treinamento.

1) Elementos de Gamificação

Elementos principais incluem [18]:

- **Pontos**: Recompensas numéricas por atividades (ex: completar módulo = 10 pontos)
- **Badges/Medalhas**: Conquistas visuais (ex: "Especialista em Phishing" após 5 simulações corretas)
- **Leaderboards**: Ranking visível de progresso (ex: top 10 servidores com consciência mais alta)
- **Níveis/Progressão**: Avanço em dificuldade (ex: Novato $\rightarrow$ Intermediário $\rightarrow$ Avançado)
- **Narrativa/Contexto**: História que engaja aprendiz (ex: "Você é agente de segurança investigando ataque")
- **Feedback imediato**: Resposta instantânea (ex: "Correto! +10 pontos")
- **Desafios**: Objetivos específicos (ex: "Identifique 3 emails phishing em 5 minutos")

2) Impacto Comprovado na Motivação e Engajamento

Dados empíricos mostram impacto significativo [18]:

- **Aumento de 51.4% em consciência cibernética**: Estudo demonstrou aumento mensurável em conhecimento de segurança quando gamificação integrada
- **Maior participação**: Abordagens gamificadas geram maior taxa de conclusão de treinamentos
- **Engajamento sustentado**: Participantes com gamificação retornam regularmente, não apenas completam uma vez
- **Redução de queda (dropout)**: Taxa de abandono de programas gamificados é significativamente menor
- **Motivação intrínseca**: Gamificação ativa motivação intrínseca (fazer porque é interessante) além de extrínseca

Particularmente, estudos mostraram que gamificação combinada com microlearning é especialmente efetiva para reduzir ansiedade e aumentar engajamento [25].

3) Quando Gamificação É Efetiva e Quando Não É

Gamificação funciona bem em:

- Treinamento obrigatório: quando participação não é opcional, gamificação torna experiência menos chata
- Conteúdo que requer prática repetida: pontos e badges incentivam repetição, crítica para retenção
- Públicos competitivos: leaderboards funcionam com grupos que respondem a comparação social
- Conteúdo modular: gamificação funciona melhor com pequenas unidades que podem ser "conquistadas"

Gamificação pode ser problemática em:

- Públicos aversivos a competição: alguns indivíduos (particularmente algumas culturas) acham competição pública desmotivante
- Pressão excessiva: leaderboards públicas podem criar ansiedade em alguns
- "Jogo de apenas ganhar": se gamificação é superficial (apenas pontos sem conexão a aprendizado real), perde efetividade [18]
- Falta de significado: se badges e pontos não conectam a valor real, perdem impacto motivacional

Importante: gamificação não substitui conteúdo bom. Um conteúdo mal desenhado não passa a ser bom apenas por utilizar a gameficação.

3.4 Simulações e Aprendizado Experiencial

Simulações, particularmente campanhas educativas de phishing, oferecem aprendizado através da experiência.

1) Simulações de Ataque Realistas

Campanhas de phishing educativo: Envios controlados de emails phishing realistas para medir quantos usuários clicam em links ou baixam anexos. Quando usuário "falha", é redirecionado para treinamento sobre o que fazer. Dados mostram essas campanhas são altamente efetivas: estudos demonstram redução em cliques quando combinadas com treinamento [18].

Simuladores: Plataformas que simulam cenários de segurança (ex: "Você é operador de rede. Detecte anomalia em padrão de tráfego").

Cenários de resposta a incidente: Exercícios onde equipes praticam resposta a simulação de violação.

2) Por Que Aprendizado Experiencial Funciona

Aprendizado experiencial [23] é ciclo: Experiência Concreta → Reflexão → Conceituação → Experimentação Ativa → nova Experiência. Simulações colocam aprendiz neste ciclo, não apenas em palestra.

Quando alguém clica em email phishing em simulação, experiência é concreta e imediata. Reflexão ("Como eu deveria ter visto isto?") leva a conceituação ("Estes são sinais de phishing"). Experimentação ativa na próxima simulação aplica conceituação. Este ciclo produz retenção e mudança comportamental superior a aprendizado passivo.

3) Crítica Importante: Abordagem Educativa vs. Punitiva

Questão crítica é: Como tratar quem "falha" em simulação?

Abordagem Punitiva (contraindicada):

- Enviar email público de vergonha
- Punição disciplinar
- Nomes publicados de quem clicou
- Resultado: Reduz reporte futuro de phishing, aumenta "esconder erro", reduz confiança

Abordagem Educativa (recomendada):

- Redirecionamento imediato para treinamento ("Você clicou. Aqui está porque era phishing e o que fazer")
- Feedback construtivo ("Melhore identificando o domínio falso")
- Reconhecimento de quem identifica e report phishing
- Resultado: Aumenta aprendizado, aumenta futuros reportes, cria ambiente seguro para admitir erro

Abordagem educativa reconhece que erro é oportunidade de aprendizado, e não alvo de punição.

3.5 Modelos Multimodais de Entrega

Nenhuma modalidade única é ótima para todos. Combinação de modalidades (blended learning) produz melhores resultados.

1) Comparação de Modalidades

2) Evidência de Superioridade de Blended Learning

Pesquisa sistemática demonstra que combinar modalidades produz: maior retenção (combinação de múltiplos canais produz reforço - aprendiz vê informação de diferentes ângulos), maior engajamento (variedade previne tédio), acessibilidade aumentada (diferentes pessoas preferem diferentes modalidades), e flexibilidade (aprendiz escolhe modalidade conforme contexto) [18].

Modalidade	Vantagens	Limitações
E-learning	Flexibilidade, escala, qualquer hora/lugar	Menor engajamento, sem perguntas em tempo real, impessoal
Presencial	Interação, perguntas respondidas, relação pessoal	Caro, deslocamento, difícil escalar
Microlearning	Retenção superior, acessível, integra bem	Insuficiente isoladamente, conhecimento fragmentado
Gamificação	Engajamento, motivação, retenção	Design complexo, pode banalizar tópicos sérios
Simulações	Aprendizado experiencial, mudança comportamental	Requer recursos, pode gerar ansiedade
Vídeo	Engajador, versatilidade	Produção complexa, risco de passividade
Texto/Leitura	Flexibilidade de ritmo, profundidade	Menor engajamento, requer literacia

Tabela I
COMPARAÇÃO DE MODALIDADES EDUCACIONAIS

Estudos encontraram que combinação de presencial + online + microlearning produziu satisfação significativamente maior que qualquer modalidade isolada [24].

3) Sequenciamento de Modalidades

Evidência sugere sequenciamento efetivo [18]:

1) **Introdução presencial ou webinar**: Estabelecer contexto, criar conexão pessoal
2) **E-learning profundo**: Conteúdo detalhado para quem precisa aprofundar
3) **Microlearning**: Reforço contínuo de conceitos-chave
4) **Simulações**: Prática experiencial
5) **Gamificação**: Motivar retorno e prática contínua
6) **Suporte pós-treinamento**: Responder perguntas, escalar problemas
7) **Comunicação contínua**: Alertas sobre ameaças emergentes, histórias de sucesso, reforço

Este sequenciamento leva aprendiz de conhecimento inicial para profundidade para prática para motivação contínua.

3.6 Fatores de Sucesso em Programas de Treinamento

Além de abordagens pedagógicas, fatores organizacionais determinam sucesso.

1) Engajamento e Participação

- **Relevância percebida**: Aprendiz deve entender POR QUE. "Proteção de senha é importante porque protege dados do Estado" é melhor que apenas exigência
- **Facilitação de acesso**: Se programa requer ir a sala específica em horário específico, taxa de participação cai. Online on-demand é superior
- **Reconhecimento de esforços**: Públicos reconhecem quem participa, referências a praticantes de segurança
- **Tempo alocado**: Se organização não aloca tempo durante expediente para treinamento, taxa de conclusão é baixa

2) Suporte Organizacional

- **Tempo oficial**: Horas de trabalho dedicadas a treinamento, não esperado "fora do expediente"

- **Recursos**: Tecnologia, conteúdo, facilitadores adequadamente financiados [18]
- **Suporte de liderança**: Mensagens de executivos que reforçam importância [18]
- **Integração em rotina**: Conscientização integrada em onboarding, reuniões periódicas, comunicações

3) Avaliação e Feedback Contínuo

- **Pré e pós-avaliação**: Medir conhecimento antes e depois para demonstrar efetividade
- **Satisfação de participantes**: "Como foi a experiência?"
- **Transferência de aprendizado**: "Está mudando comportamento no trabalho?"
- **Indicadores de impacto**: Redução em incidentes relacionados a fator humano

4. MELHORES PRÁTICAS DE CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO

4.1 Levantamento Sistemático de Boas Práticas Internacionais

A implementação eficaz de programas de treinamento em conscientização sobre segurança da informação requer uma compreensão profunda das melhores práticas internacionais estabelecidas e validadas pela comunidade científica. Esta pesquisa, baseada em uma revisão sistemática da literatura, visa identificar estruturas e padrões reconhecidos globalmente.

1) Frameworks e Padrões Reconhecidos

A Organização Internacional de Normalização (ISO) fornece a estrutura mais amplamente aceita. A ISO/IEC 17799 (posteriormente renomeada ISO/IEC 27002) estabelece um conjunto de diretrizes para práticas de gestão de segurança da informação, com base em um ciclo de melhoria contínua conhecido como PDCA (Planejar-Executar-Verificar-Agir). Este ciclo permanece um método fundamental na Gestão da Qualidade Total e é particularmente recomendado para a gestão de projetos de segurança da informação [26].

A norma ISO/IEC 13335 (Diretrizes para Gestão de Segurança de Tecnologia da Informação - GMITS) descreve os conceitos e modelos básicos de gestão de segurança de tecnologia da informação. O guia recomenda especificamente a criação de um comitê interdisciplinar responsável por definir níveis de risco aceitáveis, monitorar resultados e reavaliar periodicamente projetos de segurança [26].

A Estrutura de Segurança Cibernética (CSF, na sigla em inglês), desenvolvida pelo Instituto Nacional de Padrões e Tecnologia (NIST, na sigla em inglês), gira em torno de cinco funções: identificação, proteção, detecção, resposta e recuperação. Dentro da função de "proteção", a conscientização do usuário é um elemento-chave reconhecido internacionalmente [18].

O COBIT (Objetivos de Controle de Tecnologia da Informação e Tecnologias Relacionadas) fornece uma estrutura de governança e gestão de tecnologia da informação, estabelecendo um modelo de maturidade e incluindo explicitamente a educação e a conscientização como um elemento do desenvolvimento da segurança organizacional [18].

2) Elementos-chave Identificados em Revisões Sistemáticas

A revisão sistemática da literatura recuperou 25 artigos sobre conscientização em cibersegurança publicados entre 2019 e 2023 [18]. A partir desses artigos, podemos resumir alguns elementos-chave de programas eficazes de cibersegurança:

Comunicação e Engajamento da Liderança: Programas de cibersegurança bem-sucedidos são caracterizados pelo envolvimento explícito da liderança. Líderes que demonstram pessoalmente seu compromisso com a cibersegurança melhoram a adesão entre seus subordinados. A alocação aberta de recursos de segurança reflete o nível de comprometimento de uma organização com a cibersegurança. Pesquisas mostram que organizações com envolvimento explícito da alta administração apresentam taxas de adesão significativamente maiores [12].

Conteúdo Estruturado e Relevante: Programas eficazes de cibersegurança diferenciam o conteúdo com base no nível de conhecimento do público (básico, intermediário, avançado) e na função profissional, fornecendo conteúdo personalizado. Pesquisas sistemáticas mostram que a personalização do conteúdo com base no nível de habilidade melhora a eficácia do programa em comparação com abordagens genéricas [12].

Abordagem Multimodal: Uma revisão de 25 modelos inovadores de treinamento demonstra a superioridade de uma abordagem multimodal [18]. Como mencionado anteriormente, a microaprendizagem apresenta excelente retenção de conhecimento, os cursos em vídeo oferecem flexibilidade, os workshops presenciais proporcionam interatividade e a gamificação aumenta o engajamento. Nota importante: O aprendizado híbrido é superior a qualquer abordagem isolada.

Reforço Contínuo: Estudos sobre a curva do esquecimento mostram que a falta de reforço leva a uma diminuição significativa na retenção de conhecimento. A conscientização sobre segurança proporciona apenas efeitos de aprendizado de curto prazo, a menos que haja prática repetida [3]. Campanhas temáticas de conscientização, alertas sobre ameaças emergentes, integração às operações diárias da organização e reforço pós-incidente contribuem para a retenção de conhecimento. Estudos sobre a curva do esquecimento [20] demonstram que a falta de reforço leva a uma diminuição significativa na retenção de conhecimento. O reforço contínuo mantém uma melhor retenção de conhecimento em comparação com sessões de treinamento isoladas [3], [12].

Medição e Feedback: Métricas de processo (taxa de conclusão, engajamento), métricas comportamentais (taxa de sucesso da simulação, notificação de incidentes) e métricas de impacto (redução de incidentes) demonstram continuamente o valor de um projeto. A comunicação regular do progresso mantém o projeto visível e fornece uma base para o investimento contínuo de recursos [18].

3) Ciclo PDCA como Abordagem de Melhoria Contínua

Metodologia amplamente adotada repousa em ciclo PDCA (Plan-Do-Check-Act) [26]. Este ciclo não é linear mas itera-

tivo: cada iteração alimenta a próxima. Cada ciclo completo tipicamente dura 6 a 12 meses.

Fase Plan: Diagnóstico de baseline, definição clara de objetivos mensuráveis, alocação de recursos, designação de responsabilidades, definição de cronograma.

Fase Do: Implementação de atividades planejadas (treinamentos, campanhas, simulações). Importante: adaptação em tempo real conforme feedback inicial, sem esperar conclusão completa do ciclo.

Fase Check: Coleta sistemática de indicadores, análise de conformidade, identificação de desvios e causas.

Fase Act: Análise de causas raízes de desvios, reajustes na estratégia (conteúdo, frequência, formato, canais), planejamento do próximo ciclo incorporando aprendizados.

4.2 Componentes Essenciais de Programas Efetivos

A análise abrangente da revisão do sistema identificou cinco elementos recorrentes em projetos comprovadamente eficazes [18]:

1) Comunicação e Engajamento da Liderança

Se um projeto não conseguir o comprometimento da liderança, ele se torna meramente um "departamento de operações", desconectado da tomada de decisões estratégicas. O comprometimento pode ser obtido por meio de: (1) comunicação repetida da importância da segurança ao público; (2) liderança pelo exemplo, demonstrando práticas seguras; (3) definição clara das alocações orçamentárias; (4) agendamento de sessões formais de treinamento; e (5) reconhecimento público da conformidade [12].

Nota importante: A comunicação deve vincular a segurança a objetivos organizacionais mais amplos, em vez de tratá-la como um requisito obrigatório.

2) Conteúdo Estruturado e Relevante

Um estudo com 24 perguntas sobre escalas de conscientização identificou nove dimensões-chave para uma conscientização eficaz [12]:

1) Gerenciamento de Senhas: Crie senhas fortes, troque-as regularmente e não as compartilhe com outras pessoas.
2) Uso de Mídias Sociais: Não acesse mídias sociais durante o horário de trabalho e não publique informações confidenciais.
3) Uso de E-mail: Não clique em links de remetentes desconhecidos e não baixe anexos suspeitos.
4) Uso da Internet: Acesse apenas sites legítimos; não insira informações pessoais.
5) Acesso e Processamento de Dados: Não exiba materiais sensíveis em locais visíveis; verifique sua autenticidade.
6) Notificação de Incidentes: Denuncie comportamentos suspeitos, violações e vazamentos de dados.
7) Segurança do Dispositivo: Mantenha o software atualizado, configure o bloqueio automático e use senhas.
8) Uso de Dispositivos Móveis: Esteja ciente de possíveis espionagens; não deixe os dispositivos sem supervisão.
9) Conhecimento das Políticas: Compreenda a responsabilidade pessoal e familiarize-se com as políticas relevantes.

O conteúdo deve ser progressivo (do básico ao avançado) e adaptado às necessidades de diferentes públicos.

3) Entrega Multimodal

Como discutido na seção anterior sobre modelos de aprendizagem, combinar múltiplas modalidades de ensino é mais eficaz do que um único método [18]. Cada modalidade tem suas vantagens: o aprendizado online oferece flexibilidade e escalabilidade, o aprendizado presencial proporciona interatividade, a microaprendizagem proporciona melhor retenção de conhecimento e o aprendizado gamificado proporciona engajamento. A simulação proporciona aprendizagem experiencial.

Abordagens multimodais integram esses elementos em uma sequência coordenada, em vez de apresentá-los isoladamente.

4) Reforço Contínuo

Retenção de conhecimento sem reforço decai rapidamente [3]. Estratégias de reforço incluem: (1) campanhas temáticas mensais ou trimestrais, (2) alertas sobre ameaças emergentes, (3) integração em rotina (e-mail corporativo, intranet, reuniões de equipe), (4) reforço pós-incidente quando comportamento inadequado é identificado [12].

Importante: reforço deve variar em formato para manter engajamento, não tornando-se repetitivo.

5) Mensuração e Feedback

Indicadores devem ser acompanhados regularmente [18]:

Indicadores de Processo: Taxa de conclusão de treinamentos, frequência de campanhas, número de simulações realizadas

Indicadores de Comportamento: Taxa de acerto em simulações de phishing, taxa de reporte de e-mails suspeitos, adesão observável a políticas

Indicadores de Impacto: Redução de incidentes por fator humano, redução de custo médio por incidente, melhoria em indicadores de maturidade em segurança

Comunicação periódica de progressos mantém programa visível dentro da organização.

4.3 Segmentação de Públicos e Adaptação a Contextos

1) Segmentação por Função e Conhecimento

Públicos diferentes exigem abordagens diferentes [12]:

- **Pessoal Operacional vs. Pessoal de Gestão:** O pessoal operacional precisa de conhecimento prático. Os gestores precisam entender o impacto dos incidentes e seu papel de liderança.
- **Usuários Técnicos vs. Usuários de Gestão:** Os usuários técnicos precisam de conhecimento sobre segurança no desenvolvimento. Usuários da gerência precisam de conhecimento geral sobre segurança.
- **Nível de Exposição ao Risco:** Gerentes de dados financeiros precisam de maior conhecimento sobre segurança. A equipe operacional precisa de conhecimento geral sobre segurança.
- **Nível de Conhecimento Prévio:** Novos usuários precisam de treinamento básico. Usuários experientes precisam de treinamento avançado sobre o tema.

2) Adaptação a Diferentes Contextos

Realidades organizacionais variam e requerem adaptação [3]:

- **Grandes vs. pequenas unidades:** Grandes permitem programas especializados. Pequenas exigem abordagem mais genérica
- **Presenciais vs. remotos:** Equipes remotas exigem canais digitais. Equipes presenciais permitem workshops
- **Alta vs. baixa maturidade em TI:** Organizações maduras em TI têm infraestrutura de suporte. Organizações menos maduras exigem soluções mais simples
- **Contexto público vs. privado:** Setor público enfrenta pressões orçamentárias e estruturas hierárquicas distintas. Setor privado pode oferecer incentivos diferenciados

3) Progressão de Maturidade

Organizações não saltam diretamente para programas maduros. Modelo de maturidade oferece estrutura de progressão [26]:

- **Nível 1 (Ad hoc):** Conscientização não estruturada, reativa
- **Nível 2 (Repetível):** Algumas atividades estruturadas, mas inconsistentes
- **Nível 3 (Definido):** Programa estruturado, documentado, aplicado consistentemente
- **Nível 4 (Gerenciado):** Programa medido, indicadores acompanhados, ajustes sistemáticos
- **Nível 5 (Otimizado):** Melhoria contínua, inovação, adaptação a novas metodologias

Progressão gradual através de níveis permite consolidação e evita regressão quando recursos são realocados.

4.4 Diagnóstico do Contexto de Setor Público

Características Estruturais Identificadas:

O setor público brasileiro possui quatro características principais que influenciam a eficácia de projetos de conscientização [3], [27]:

1) **Estrutura Hierárquica Formal e Estruturada:** Diferentemente do setor privado, mais flexível, a estrutura do setor público é vertical. A comunicação de cima para baixo é apropriada e eficaz. Tentativas de "democratizar" as decisões de segurança frequentemente levam à paralisia ou inconsistência [27].
2) **Ciclos Políticos e Descontinuidade Administrativa:** Mudanças na gestão reduzem a sustentabilidade de projetos não institucionalizados. Isso torna necessária a regulamentação da conscientização pública por meio de documentos obrigatórios (leis, regulamentos), em vez de depender de uma gestão administrativa específica [27].
3) **Restrições Orçamentárias de Longo Prazo:** Acesso limitado a "ferramentas avançadas". Isso nos força a adotar um modelo simplificado: o microaprendizado via e-mail corporativo (sem custo) é superior ao aprendizado online baseado em SaaS [3].
4) **Orientação para Objetivos em vez de Remuneração:** Servidores públicos são frequentemente motivados por um senso de "servir à sociedade" e "missão institucional", em vez de incentivos econômicos. Isso faz com que suas âncoras emocionais sejam diferentes: "Garantir a segurança dos dados dos cidadãos" ressoa mais do que "evitar multas com segurança" [27].

Vulnerabilidades Comportamentais Específicas:

Análise ergonômica em instituição pública federal identificou dois padrões críticos [3]:

1) **Conflito entre prescrição de trabalho e prescrição de segurança:** Servidor enfrenta pressão de cumprir objetivo de trabalho (urgente, visível) enquanto segue política de segurança (preventiva, invisível). Sob pressão, servidor frequentemente escolhe violar segurança. Não é falta de integridade, é conflito genuíno de prescrições.
2) **Pressão temporal reduzindo conformidade:** Quando deadline se aproxima, segurança é preterida racionalmente (risco improvável vs. consequência certa de perder deadline). Isto demanda conscientização integrada em fluxo de trabalho, não apresentada como "passo adicional".

Características Positivas a Explorar:

1) **Estabilidade de força de trabalho:** Servidores públicos têm permanência contratual garantida, frequentemente superando uma década na mesma instituição [19]. Em contraste, setor privado apresenta maior rotatividade de pessoal, tornando o investimento em conscientização de servidores públicos particularmente significativo, dado que conhecimentos e comportamentos de segurança perduram ao longo de carreiras mais estáveis.
2) **Solidariedade coletiva:** Pesquisa transcultural mostrou que contextos públicos com hierarquia formalizada também apresentam identidade coletiva forte [19]. Isto permite gamificação e reconhecimento coletivo, não individual.

4.5 Implicações Estratégicas para Modelo Proposto

Diagnóstico acima fundamenta quatro requisitos críticos que modelo de conscientização em setor público DEVE contemplar:

Requisito 1 - Formalização Obrigatória com Longevidade Administrativa:

Fraqueza de ciclos políticos exige que programa resulte em documentação formal (portaria, instrução de serviço) que delineia responsabilidades, cronograma, e sanções. Isto institucionaliza programa e permite continuidade além de mudanças administrativas

Requisito 2 - Respeito a Hierarquia Formal com Amplificação de Mensagem:

Contrariamente a preconcepção que "bottom-up é sempre melhor", setor público responde bem a comunicação top-down quando suportada por autoridade clara. Comunicação deve ser iniciada por liderança executiva, então percolada através de canais hierárquicos formais. Isto amplifica impacto de mensagem e reforça que "segurança é prioridade institucional".

Requisito 3 - Reconhecimento de Conflitos Legítimos de Prescrição com Caminhos Intermediários:

Modelo não pode ser “puro” (nunca compartilhe senhas). Deve oferecer “alternativas intermediárias” que reconhecem pressões reais: “quando necessário compartilhar senha (situação excepcional documentada), use conta de serviço com acesso temporário (máximo 2 horas), com dupla autenticação, documentado e auditável”. Esta abordagem mantém segurança enquanto reconhece realidade do trabalho público. Paralelo: pressionar por melhoria de infraestrutura TI que reduz necessidade de violação.

Requisito 4 - Integração em Fluxo de Trabalho com Pontualidade e Contexto:

Conscientização deve ser integrada no dia-a-dia, não apresentada como “passo adicional” que reduz produtividade. Isto requer:

- Microlearning breve (7-10 minutos) oferecido durante “tempo livre” (café da manhã via celular), não blocos de 2 horas
- Lembretes contextualizados ao problema específico que servidor está resolvendo (não generic)
- Automação de segurança (bloqueio automático em 5 minutos em vez de “lembre-se de bloquear”)
- Explorar motivação por propósito: “você está protegendo dados que cidadão confiou a nosso país” é mais poderoso que “você está seguindo regulação”.

5. OPERACIONALIZAÇÃO DA CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO

5.1 Visão Geral do Programa de Conscientização em Segurança da Informação

A conscientização em segurança da informação não é fim em si, mas transformação de conhecimento em comportamento duradouro e conforme. A seção anterior estabeleceu as melhores práticas internacionais fundamentadas em frameworks como PDCA, componentes essenciais e modelos de segmentação. A seção 3 estabeleceu a pedagogia efetiva através de microlearning, gamificação e multimodalidade. Esta seção operacionaliza estas descobertas através de um modelo integrado de conscientização para o Ministério da Fazenda, com foco em premissas estruturantes e requisitos do programa.

5.2 Premissas Estruturantes

1) Premissa 1: Consciência Não é Conformidade

Conhecimento educacional não implica automaticamente em comportamento. Conscientização isolada produz uma retenção inadequada, sem reforço contínuo. Transformação de consciência em conformidade requer integração multidimensional entre educação (transferência de conhecimento), política de segurança (clarificação de expectativas), tecnologia (habilitação de comportamento) e cultura organizacional (normalização de práticas seguras) [18].

Implicação: O programa não é treinamento. É transformação comportamental estruturada.

2) Premissa 2: Contexto Público Requer Pragmatismo

Existe um debate real entre o que uma tarefa precisa (a forma de fazer rápido) e o que é texto seguro. Muitas vezes, os servidores e colaboradores pulam partes importantes para proteger a si mesmos. Ideais sobre segurança: Em pouco tempo, os sistemas falham. A ideia de pragmatismo ajuda as pessoas a acharem formas de achar um jeito do meio que mantivesse todo mundo seguro mas sem perder o trabalho; Ela é muito importante para o lugar onde se trabalha.

Implicação: A política reconhece exceções documentadas. O conteúdo oferece estratégias realistas, não ideais.

3) Premissa 3: Reforço Contínuo é Não-Negociável

Retenção de conhecimento mantém-se significativamente superior quando implementados mecanismos de reforço contínuo comparado àquela observada em treinamentos isolados. O espaçamento temporal de revisões supera concentração em sessão única. Conforme demonstrado por Ebbinghaus [20], sem revisão sistemática, pessoas esquecem aproximadamente 50% da informação após uma hora, 70% após vinte e quatro horas, e 90% após uma semana [24]. Consequentemente, um programa que oferece conscientização inicial sem reforço contínuo inevitavelmente apresentará regressão em retenção de conhecimento.

Implicação: O programa é permanente, não uma campanha sazonal. O reforço deve ser mensal, no mínimo.

4) Premissa 4: Escala Requer Ferramenta Centralizada

Restrições orçamentárias do setor público exigem eficiência. Restrições de força produtiva da equipe exige uma solução que diminua esse ponto. Escala dentro da organização requer padronização de conteúdo. Modelos baseados exclusivamente em instrutor não escalam adequadamente. Uma ferramenta centralizada permite escalabilidade, consistência, reforço automático e mensuração centralizada.

Implicação: Uma plataforma ou ferramenta é fonte primária de conscientização.

5) Premissa 5: Indicadores Validam Impacto

Sem mensuração, o programa é invisível e vulnerável ao abandono. Indicadores em três camadas (processo, comportamento, impacto) validam execução conforme plano, mudança real em segurança e valor do investimento.

Implicação: Mensuração não é opcional, é validação do programa.

5.3 Requisitos Críticos do Programa

1) Requisito 1: Formalização e Permanência

O programa deve ser institucionalizado através de instrumento formal que garanta continuidade além de ciclos administrativos. Responsabilidades devem ser atribuídas a cargos, não a pessoas. O programa deve integrar-se à estrutura de governança estabelecida (CGSP-MF, SSI-MF) e constar de planejamento plurianual.

2) Requisito 2: Pedagogia Multimodal com Gamificação

O programa deve operacionalizar metodologias comprovadas: microlearning como modalidade primária (7-10 minutos), gamificação integrada (badges, pontos, reconhecimento), simulações experienciais (phishing educativo) e reforço contí-

nuo estruturado. Uma ferramenta centralizada deve ser o meio para entrega de conteúdo e mensuração.

3) Requisito 3: Reconhecimento de Realidade Operacional

O programa deve oferecer caminhos intermediários para dilemas reais do contexto (compartilhamento urgente de credenciais, software não disponível, pressão de prazo). Exceções devem ser documentadas e auditadas. Conteúdo deve estar integrado aos fluxos de trabalho existentes.

4) Requisito 4: Escalabilidade com Segmentação

O programa deve oferecer conteúdo segmentado por público (onboarding, função específica, nível de conhecimento) e suportar progressão gradual de maturidade. Diferentes públicos avançam em ritmo apropriado sem comprometer o todo.

5) Requisito 5: Engajamento de Liderança

O programa deve contar com comunicação formal de liderança executiva reforçando importância, cascata através de hierarquia formal, modelagem de comportamentos seguros e integração em responsabilidades de gestão.

6) Requisito 6: Mensuração Contínua

O programa deve estabelecer indicadores em três camadas: processo (execução: cobertura, conclusão, conformidade de reporte), comportamento (mudança real: computadores desbloqueados, cliques em phishing, reporte de incidentes), impacto (resultado: incidentes por fator humano reduzidos, maturidade em segurança evoluída). Ciclo contínuo de verificação e ajuste deve ser estabelecido.

5.4 Arquitetura do Programa

1) Componente 1: Ferramenta Centralizada de Conscientização

A ferramenta é a base para entrega e mensuração de conscientização. Ela deve suportar: microlearning em módulos de 7-10 minutos, gamificação com badges e reconhecimento de progresso, simulações de phishing com educação imediata para usuários que clicam, segmentação de conteúdo por tipo de público (onboarding, função operacional, função gerencial, função técnica, função administrativa de dados), algoritmo de espaçamento para revisão programada de tópicos críticos, e geração de relatórios sobre indicadores de processo, comportamento e impacto.

A ferramenta pode ser solução de mercado reconhecida ou desenvolvida internamente, desde que cumpra os requisitos acima.

2) Componente 2: Estrutura de Governança

A governança opera em três níveis:

Nível Estratégico (CGSP-MF, com auxílio do SSI-MF): Aprovação de política de conscientização, alocação de recursos, revisão anual de impacto.

Nível Operacional (Gestor de Segurança da Informação): Governança mensal de execução, aprovação de conteúdo adicional, revisão de indicadores, recomendações de ajuste.

Nível de Execução: Gestor de Segurança da Informação e equipe coordena centralização, integração com ferramenta, alinhamento de conteúdo; Responsáveis de Segurança da Informação por área implementam localmente, adaptam conteúdo e engajam liderança local.

3) Componente 3: Estrutura de Conteúdo

O conteúdo é segmentado em quatro categorias:

Onboarding: 4-6 horas (combinação de e-learning assíncrono e remoto ao vivo), obrigatório para novos servidores nos primeiros 30 dias. Cobre políticas de segurança, vulnerabilidades básicas, procedimentos de resposta a incidente.

Por Função: Conteúdo adaptado a papéis específicos, de acordo com a sua função na estrutura do Ministério ou sua atuação operacional(boas práticas diárias, reconhecimento de phishing, gestão de senhas), servidores em posições de chefia (responsabilidade em criar cultura, comunicação com subordinados), servidores e colaboradores (segurança em desenvolvimento, análise de risco), administrativos de dados (conformidade LGPD, acesso a informações sensíveis, segregação de responsabilidades).

Dilemas Realistas: Módulos de 10-15 minutos abordando conflitos específicos identificados no contexto (compartilhamento urgente de credenciais, software não disponível, pressão temporal). Estes módulos oferecem caminhos intermediários que mantêm segurança sem sacrificar produtividade.

Reforço Estruturado: Microlearning semanal via ferramenta (8-10 minutos), simulação de phishing mensal com educação imediata, workshop trimestral presencial (2 horas).

4) Componente 4: Reconhecimento de Realidade Operacional

O programa formaliza exceções autorizadas. Cada exceção deve especificar: situações em que é autorizada, salvaguardas (dupla autenticação, duração máxima, auditoria), como se registra. Fluxos de trabalho são redesenhados para permitir conformidade sob pressão — por exemplo, requisição urgente de software analisada em 5 dias úteis (versus fila normal de meses), com alternativas seguras comunicadas quando rejeitadas.

5) Componente 5: Mensuração

Indicadores de Processo: Cobertura de conscientização (% de servidores que receberam conteúdo, meta 100%), conclusão de onboarding (% de novos que completaram em 30 dias, meta 100%), conformidade de reporte (% de áreas que submeteram indicadores no prazo, meta 100%).

Indicadores de Comportamento: Computadores desbloqueados em varredura de segurança (redução de 45% para 20%), cliques em phishing simulado (redução de 25% para 8-10%), reporte proativo de incidentes (aumento de 30% para 60%), conformidade auditada (aumento de 30% para 70%).

Indicadores de Impacto: Número de incidentes atribuíveis a fator humano (redução de 12/ano para 6/ano no Ano 1), evolução de maturidade em segurança (progressão de Nível 2 para Nível 3).

Cadência de Análise: Mensal (Gestor de SI coleta dados, identifica desvios, recomenda ajustes táticos), trimestral (Gestor de SI analisa tendências e escalações), anual (CGSP-MF revisa impacto e recomenda continuação/evolução).

5.5 O Que o Programa Não É

O programa não inclui: infraestrutura técnica (responsabilidade de MGI, através do ColaboraGov), customização

extrema por unidade, punição por não-conformidade educativa, campanhas com término definido, conscientização isolada de conformidade e cultura organizacional.

6. Conclusão e Trabalhos Futuros

A conscientização em segurança da informação emerge, através desta pesquisa, não como componente isolado, mas como pilar integrado e estrutural da governança de segurança da informação. A segurança da informação no setor público brasileiro é desafio que transcende tecnologia. É desafio primariamente de conhecimento, comportamento e cultura. Programas estruturados de conscientização — fundamentados em evidência científica, implementados através de pedagogia comprovada, operacionalizados através de governança robusta — representam investimento não apenas defensivo, mas multiplicador de maturidade de segurança da informação.

6.1 Síntese de Achados Principais

Este trabalho consolidou a compreensão de conscientização através de três dimensões complementares:

Primeira Dimensão: Centralidade do Fator Humano. A revisão sistemática da literatura confirmou que incidentes relacionados a erro humano constituem entre 85% e 95% do total de incidentes de segurança em organizações públicas e privadas [12]. Vulnerabilidades de comportamento (senhas fracas, compartilhamento de credenciais, cliques em phishing) representam vetor de ataque não apenas mais frequente, mas economicamente explorado. Análise de frameworks internacionais (NIST Cybersecurity Framework, ISO 27001, COBIT) e normativa brasileira (LGPD, Portaria GSI/PR 915/2022, Decreto 10.677/2021) convergem para estabelecer conscientização como requisito mandatório de conformidade, não recomendação opcional [28].

Segunda Dimensão: Pedagogia Cientificamente Comprovada. Aplicação de princípios pedagógicos fundamentados em andragogia [22], ciclo experiencial de aprendizado [23] e spacing effect de retenção [20] revelou que efetividade não é inerente ao conteúdo, mas à sua estrutura de entrega. Microlearning (7–10 minutos) combinado com reforço espaçado e gamificação integrada produz retenção e mudança comportamental substantivamente superior [18], [21], [24]. Multimodalidade — combinação de e-learning, presencial, simulações e reforço contínuo — emerge como necessária, não como algo adicional. Retenção sem reforço estruturado é inadequada: 50% após 24 horas, 90% após uma semana conforme modelo de Ebbinghaus documentado em revisão sistemática.

Terceira Dimensão: Operacionalização Pragmática Sustentável. Efetividade requer não apenas conteúdo pedagógico, mas formalização normativa que garanta continuidade institucional, centralização tecnológica que viabilize escalabilidade [18], e mensuração contínua que valide impacto. Reconhecimento pragmático de dilemas reais entre segurança ideal e produtividade — com formalização de exceções documentadas — aumenta viabilidade e aceitação geral. Mensuração em três camadas (processo, comportamento, impacto) fornece base para otimização contínua, conforme evidência de efetividade de programas estruturados em organizações públicas [12].

6.2 Contribuições e Reposicionamento

Ao conhecimento científico: síntese sistemática de evidências sobre fator humano em segurança; aplicação de frameworks pedagógicos ao contexto de segurança da informação; desenvolvimento de modelo operacional que articula governança, pedagogia e tecnologia.

À Administração Pública Federal: modelo estruturado para implementação no Ministério da Fazenda e órgãos da Administração Pública Federal; diretrizes específicas para contexto público; guia para seleção e implementação de ferramenta centralizada; requisitos funcionais de programa; e indicadores para mensuração.

À governança de segurança da informação: reposicionamento de conscientização de atividade periférica para componente estrutural de governança, demonstrando que efetividade depende de integração com estruturas existentes (CGSP, SSI, Responsáveis de SI), formalização normativa e mensuração integrada.

6.3 Trabalhos Futuros

Pesquisa futura pode aprofundar este trabalho em dimensões específicas:

Pesquisa Operacional: Estudo experimental no Ministério da Fazenda comparando efetividade relativa de modalidades pedagógicas em amostra controlada de servidores públicos brasileiros. Investigação sobre relação entre perfis (idade, experiência técnica, estilos de aprendizado) e efetividade de modalidades, permitindo personalização de entrega. Estudo longitudinal acompanhando retenção comportamental ao longo de 6–12 meses pós-programa, validando modelos de espaçamento.

Expansão Operacional: Piloto no Ministério da Fazenda em unidade específica para validação de modelo em contexto real. Replicação gradual para órgãos da Administração Pública Federal com ajustes contextuais. Desenvolvimento de conteúdo microlearning segmentado por funções específicas da organização. Seleção, customização ou desenvolvimento de ferramenta tecnológica centralizada que implemente requisitos propostos.

Evolução Metodológica: Exploração de capacidades de inteligência artificial para personalização adaptativa de conteúdo em tempo real baseada em desempenho individual. Análise comportamental agregada para identificação de padrões de risco e customização de intervenções. Evolução de simulações educativas para ambientes mais realistas que replicam fluxos de trabalho reais.

6.4 Consideração Final

Acredita-se que o modelo proposto neste trabalho oferece um caminho concreto e baseado em evidências para transformar a realidade de segurança da informação no Ministério da Fazenda. Sua implementação, caso bem-sucedida, não apenas reduzirá vulnerabilidades causadas por erro humano, mas

criará cultura organizacional na qual segurança da informação passa a ser responsabilidade compartilhada e contínua. Dessa forma, concluí-se que a conscientização em segurança da informação emerge não como custo a ser minimizado, mas como investimento estratégico em capacidade institucional, resiliência organizacional e conformidade regulatória.

Referências

[1] R. N. Alves, J. M. H. Alves, and I. O. Vasconcelos, "Fator humano na segurança da informação: um mapeamento dos comportamentos de risco no ambiente digital."

[2] Polícia Federal do Brasil, "Operação gold digger: Pf combate organização criminosa especializada em invasão de dispositivos informáticos e desvio de dinheiro público," Aug. 2024, comunicado Oficial. [Online]. Available: https://www.gov.br/pf/pt-br/assuntos/noticias/2024/agosto/pf-combate-organizacao-criminosa-especializada-em-invasao-de-dispositivos-informaticos-e-desvio-de-dinheiro-publico

[3] R. B. D. Santos and T. B. P. E. Silva, "Gestão da segurança da informação e comunicações: análise ergonômica para avaliação de comportamentos inseguros," *RDBCI Revista Digital de Biblioteconomia e Ciência da Informação*, vol. 19, p. e021024, Oct. 2021. [Online]. Available: https://periodicos.sbu.unicamp.br/ojs/index.php/rdbci/article/view/8665529

[4] Presidência da República, "Decreto nº 9.637, de 26 de dezembro de 2018 — institui a política nacional de segurança da informação (pnsi)," Diário Oficial da União, 2018, disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm Acesso em: 24 nov. 2025.

[5] ——, "Lei nº 13.709, de 14 de agosto de 2018 — lei geral de proteção de dados pessoais (lgpd)," Diário Oficial da União, 2018, disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm Acesso em: 24 nov. 2025.

[6] Gabinete de Segurança Institucional da Presidência da República, "Estratégia nacional de segurança cibernética (e-ciber) — 2020-2023," 2019, disponível em: https://www.gov.br/gsi/pt-br/assuntos/ciberseguranca/estrategia-nacional-de-seguranca-cibernetica-e-ciber Acesso em: 24 nov. 2025.

[7] C. Rândau, "Information security challenges in organizations," 2018.

[8] A. Alsharif *et al.*, "Impact of human vulnerabilities on cybersecurity," 2022.

[9] K. Mohammed *et al.*, "Locked the car, why not the computer?" 2021.

[10] E. K. Szczepaniuk and H. Szczepaniuk, "Analysis of cybersecurity competencies and awareness," 2022.

[11] Governo Federal do Brasil, "Decreto n° 11.837, de 21 de dezembro de 2023," Dec. 2023, institui o Centro de Serviços Compartilhados - ColaboraGov. [Online]. Available: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11837.htm

[12] R. Rohan, D. Pal, J. Hautamäki, S. Funilkul, W. Chutimaskul, and H. Thapliyal, "A systematic literature review of cybersecurity scales assessing information security awareness," *Heliyon*, vol. 9, no. 3, p. e14234, Mar. 2023. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S240584402301441X

[13] E. Albrechtsen and J. H. Hovden, "Managing information security compliance: How to develop awareness and cultural change," *Information Management Computer Security*, vol. 18, no. 1, pp. 31–43, 2010.

[14] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. J. D. P. Jerram, "Determining employee awareness using the human aspects of information security questionnaire (hais-q)," *Computers Security*, vol. 42, pp. 165–176, 2014.

[15] T. Team. (2023) Security awareness training. Acesso em: 24 nov. 2025. [Online]. Available: https://www.todyl.com/blog/why-businesses-need-security-awareness-trainings

[16] D. Secure. (2025) Security awareness & culture: Defense-grade training for every organization. Acesso em: 24 nov. 2025. [Online]. Available: https://www.dragnetsecure.com/blog/security-awareness-culture-defense-grade-training-for-every-organization

[17] L. Corporation. (2023) E&c platform | catalyst by lrn. Acesso em: 24 nov. 2025. [Online]. Available: https://lrn.com/products

[18] H. Taherdoost, "Towards an Innovative Model for Cybersecurity Awareness Training," *Information*, vol. 15, no. 9, p. 512, Aug. 2024. [Online]. Available: https://www.mdpi.com/2078-2489/15/9/512

[19] E. Riahi and M. S. Islam, "Employees' information security awareness (ISA) in public organisations: insights from cross-cultural studies in Sweden, France, and Tunisia," *Behaviour & Information Technology*, vol. 44, no. 1, pp. 79–101, Jan. 2025. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/0144929X.2024.2311734

[20] H. Ebbinghaus, *Über das Gedächtnis: Untersuchungen zur experimentellen Psychologie*. Leipzig: Duncker & Humblot, 1885, tradução em inglês: Ebbinghaus, H. (1913). *Memory: A Contribution to Experimental Psychology*. New York: Teachers College, Columbia University. [Online]. Available: https://archive.org/details/memoryaContribEbbinghausEng1913

[21] E. S. Silva, W. P. D. Costa, J. C. D. Lima, and J. C. Ferreira, "Contribution of Microlearning in Basic Education: A Systematic Review," *Education Sciences*, vol. 15, no. 3, p. 302, Feb. 2025. [Online]. Available: https://www.mdpi.com/2227-7102/15/3/302

[22] M. S. Knowles, *The Adult Learner: A Neglected Species*, 3rd ed. Houston: Gulf Publishing, 1984.

[23] D. A. Kolb, *Experiential Learning: Experience as the Source of Learning and Development*. Englewood Cliffs, NJ: Prentice Hall, 1984.

[24] N. F. Alias and R. Abdul Razak, "EXPLORING THE PEDAGOGICAL ASPECTS OF MICROLEARNING IN EDUCATIONAL SETTINGS: A SYSTEMATIC LITERATURE REVIEW," *Malaysian Journal of Learning and Instruction*, vol. 20, 2023. [Online]. Available: http://e-journal.uum.edu.my/index.php/mjli/article/view/19329

[25] L. Zarshenas, E. Saranjam, M. Mehrabi, and G. Setoodeh, "Microlearning and gamification in anxiety management among girl adolescents in iran: An interventional study," *Pakistan Journal of Medical Health Sciences*, vol. 14, no. 1, pp. 689–693, 2020. [Online]. Available: https://pjmhsonline.com/2020/jan_march/pdf/n/689.pdf

[26] C. A. S. S. Martins, Alaíde Barbosa, "JOURNAL OF INFORMATION SYSTEMS," *Journal of Information Systems and Technology Management*, vol. 2, no. 2, 2005.

[27] M. R. D. S. Camões, A. D. O. Gomes, B. Rizardi, and J. Lemos, "Os ciclos de engajamento no trabalho de servidores públicos federais," *Revista de Administração Pública*, vol. 57, no. 4, pp. e2023–0061, Jul. 2023. [Online]. Available: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0034-76122023000400502&tlng=pt

[28] F. A. Aloul, "The Need for Effective Information Security Awareness," *Journal of Advances in Information Technology*, vol. 3, no. 3, pp. 176–183, Aug. 2012. [Online]. Available: http://www.jait.us/index.php?m=content&c=index&a=show&catid=150&id=791