www.revistaft.com.br

Revista FT | ISSN 1678-08sc17 | v. 30, n. 157, 2026 | DOI: 10.69849/8qv06323

Segurança milionária, brecha de centavos

O treinamento contínuo de usuários é tão vital quanto qualquer firewall de última geração.

Million-dollar security, cent-Level vulnerability

Continuous user training is as vital as any state-of-the-art firewall.

Ana Carolina de Oliveira
Felipe Antonio de Melo Alves
Gabriel Bastos Pagamisse
Nicolas Briz de Siqueira
Sidnei Luiz da Silva Júnior
Adani Cusin Sacilotti[1]

RESUMO

Este artigo tem como objetivo abrir a discussão sobre treinamento de pessoas em visão dos ataques cibernéticos utilizando estratégias menos técnicas e mais persuasivas, será abordado mais profundamente sobre engenharia social, phishing e outros golpes. Traz-se um estudo de caso onde este erro humano trouxe consequências catastróficas a uma empresa, com o objetivo de apresentar que apesar de todas as ferramentas de segurança e firewall, o treinamento humano nessas situações é necessário para identificar e prevenir esses perigos. O artigo utiliza referências bibliográficas para apresentar, explicar e trazer entendimento com relação à importância de treinamentos para a segurança dos dados e elementos tecnológicos de organizações. Se vê necessário e prudente a conscientização das organizações a respeito dessa importância, já que é frequente encontrar casos e situações em que estas preocupações são subestimadas ou mal homologadas.

[1] orientadora

Palavras-chave: Supply Chain; BaaS; Engenharia Social; Phishing; KPI.

ABSTRACT

This article has the objective of opening a discussion about the training of people in vision of cybernetic attacks utilizing strategies with less technical aspects and a more persuasive way, it will be addressed further about social engineering, phishing and other scams. A case study is brought up, where the human mistake made catastrophic consequences to a company, with the objective to present that although all the security tools and firewall, human training in these situations is necessary to identify and prevent such dangers. The article utilizes bibliographic references to show, explain and bring understanding about the importance of practices for data security and technological elements of companies. Is seen as necessary and prudent for institutions to raise awareness regarding this importance, given that it is common to find instances and situations in which those worries are underestimated or poorly approved.

Keywords: Supply Chain; BaaS; Social Engineering; Phishing; KPI.

1 INTRODUÇÃO

O pilar estratégico das organizações contemporâneas, a Segurança da Informação recebe altos investimentos em sua criação, manutenção e aplicação, Weigert e Castilho Júnior (2017) ressaltam que apesar de essenciais não aplicam a segurança por completo, em um mundo onde apenas detectar e monitorar não são suficientes para garantir a proteção integral dos ativos informacionais.

Conforme um estudo realizado por (DHILLON, 2004) o elo humano é o mais fraco e o mais fácil de ultrapassar, o que pode custar acesso aos mais importantes sistemas e dados de uma empresa. Isso se relaciona então que existe uma percepção perigosa dos colaboradores que traz um teor de negligência perante os

perigos apresentados com os ataques cibernéticos, onde concorda-se que o fator humano é uma barreira decisiva para barrar os ataques cibernéticos e se não possuir o acompanhamento correto e treinamento adequado, a linha de defesa “firewall humano” pode ser facilmente ultrapassada.

Este artigo tem como objetivo analisar o teor humano nas questões de defesas e ataques cibernéticos, seus níveis de complicação e a lembrança de que a capacitação dos colaboradores que podem receber tais ataques é de tamanha importância como os sistemas de segurança mais caros no mercado, assim sendo atribuído como um elemento decisivo na eficácia das estratégias de segurança com ações diárias de melhorias e monitoramento. Para isso será apresentado um estudo de caso que evidencia os reais impactos dessas falhas em grandes empresas e as táticas para aproveitar as vulnerabilidades humanas. Reforça-se com este estudo que a segurança de dados vai além dos processos técnicos, ela baseia-se em questões culturais e comportamentais, ressalvando a importância de manter-se uma equipe capacitada e alinhada às práticas e padrões de segurança, documentos, protocolos, normas e diretrizes, além de investimento em áreas de gestão de acesso privilegiado e identidade e acesso, a fim de tornar o ambiente online corporativo em um local mais seguro e comprometido com a confidencialidade e integridade de dados dos clientes.

2 INVESTIMENTO MILIONÁRIO, VULNERABILIDADE INVISÍVEL

No cenário atual das empresas e corporativos, a segurança da informação é constantemente ligada a investimentos pesados em firewalls de última geração, sistemas de detecção de intrusos e soluções avançadas de monitoramento. Apesar de serem muito importantes, essas tecnologias não são suficientes para garantir a proteção completa das organizações (WEIGERT, Alexsander; JUNIOR, Gelásio O. C., 2017).

Existem milhares de possíveis vulnerabilidades baseadas na confiança sem hesitância na tecnologia e seus responsáveis dentro da empresa. Entre elas, é possível citar algumas: falhas de configuração em servidores e dispositivos de rede, vulnerabilidades conhecidas em softwares que não foram devidamente corrigidas, ataques de negação de serviço distribuído (DDoS), exploração de aplicações web não seguras e a prática do Shadow IT, em que colaboradores utilizam aplicações ou

dispositivos não homologados. O foco excessivo na tecnologia ignora a vulnerabilidade humana, que Dhillon (2004) coloca como essencial, abrangendo a ética, a confiança e a honestidade, além dos pilares técnicos de confidencialidade e integridade.

Não basta ter sistemas robustos: as pessoas e a cultura da organização precisam ser parte da proteção. Esse elemento principal, o fator humano, agindo como um firewall humano, é frequentemente a maior brecha na estratégia de cibersegurança.

2.1 A brecha vulnerável: as pessoas

Autores como Schneier (2015), Pfleeger e Pfleeger (2012), e Anderson (2020) concordam que a tecnologia não substitui o julgamento humano. Acreditar que sistemas automatizados resolvem tudo é, por si só, uma vulnerabilidade. Da mesma forma, Pfleeger e Pfleeger (2012) destacam que a segurança depende da combinação entre pessoas, processos e tecnologias, e não é possível resolver tudo apenas ignorando o fator humano, isso pode ser complementado por Anderson (2020), que diz que a tecnologia ajuda a proteger, mas não substitui o julgamento e as decisões conscientes das pessoas.

Por isso, a ideia de que sistemas automatizados podem, sozinhos, garantir a segurança cibernética de uma organização é uma vulnerabilidade, por si só. E como substituir totalmente os seres humanos é inviável, o comportamento humano é explorado em ataques cibernéticos. Basta que um funcionário clique em um link perigoso, compartilhe uma senha de forma incorreta ou caia em uma tentativa de enganação para que todo o investimento em tecnologia fique comprometido. Ou seja, sem treinar bem as pessoas, até a defesa mais forte pode acabar sendo vulnerável.

O cérebro humano usa atalhos mentais que afetam como percebemos os riscos. Um exemplo é o medo de voar, comum mesmo sabendo que acidentes de avião são mais raros do que os rodoviários. Esse viés perceptivo (KAHNEMANN, Daniel, 2011) também se reflete na área de segurança digital: os colaboradores não se atentam às ameaças cotidianas, como e-mails de phishing, enquanto se preocupam com cenários menos prováveis. E por isso há a importância de programas contínuos de conscientização e treinamento, que ajudam a alinhar a

percepção dos usuários à realidade dos riscos existentes.

2.2 Incidentes comuns

Entre os incidentes mais recorrentes que envolvem falhas humanas, destacam-se três grandes desafios: o uso indevido de credenciais, o chamado *Shadow IT* e as vulnerabilidades conhecidas, mas não corrigidas.

O uso de credenciais válidas obtidas de forma ilegal é muito perigoso, porque permite que invasores se movimentem pelo ambiente da empresa quase sem serem percebidos. O *Shadow IT,* que acontece quando se usam dispositivos ou aplicativos não autorizados, também aumenta os riscos e facilita ataques. Por fim, ignorar ou tratar de forma superficial as vulnerabilidades encontradas gera uma falsa sensação de segurança, que acaba não existindo no momento de necessidade.

Além disso, o custo de um erro humano, ainda que pequeno, vai muito além de uma simples falha pontual. Ele pode incluir tempo perdido na correção, retrabalho, paralisação de sistemas, perda de informações e até danos à reputação da organização. Cada incidente desse tipo representa não apenas um gasto financeiro, mas também uma ameaça à continuidade e a confiança da empresa.

3 O FATOR HUMANO: A PORTA DE ENTRADA MAIS SUBESTIMADA

Segundo Kevin D. Mitnick (2003), mesmo quando uma empresa investe em tecnologias de segurança de ponta, treina diligentemente os funcionários e contrata seguranças, ela ainda pode permanecer vulnerável devido à exploração do fator humano na segurança da informação. O fator humano é uma das causas de intrusão em empresas mais recorrentes mesmo com o avanço da tecnologia e avanço em treinamentos em cibersegurança.

Um bom profissional com devidas competências consegue prevenir acessos indevidos e tentativas de entradas não liberadas. O treinamento para as pessoas nestas posições deve abranger vários tipos de abordagem, tanto que atualmente gestores e gerentes estão mais abertamente envolvidos nos processos e acompanhando em tempo integral todos os processos. “O ponto fraco de toda essa pirâmide está na base, no alicerce desse sistema viciado que é o próprio ser

humano.” (ALCOFORADO; RIBEIRO; CUNHA, p. 3)

3.1 Engenharia Social

Uma ciência comportamental que entende o fator humano e utiliza para realizar os ataques cibernéticos é a Engenharia Social, é uma prática onde utiliza de informações falsas ou controle das mesmas para manipular pessoas a permitirem acesso não autorizado a sistemas de informações, bancos de dados, entre outros. Segundo a Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio), Os atacantes exploram sistematicamente cinco vieses cognitivos principais: Viés da confirmação; Aversão a perda; Viés da ancoragem; Viés da disponibilidade e Viés de retrospecto.

De acordo com Mann (2011) e Thomas (2007) engenharia social utiliza muito mais entendimento do ser humano do que informações técnicas de invasão, a tentativa de entender padrões e utilizar técnicas de persuasão na hora do contato [e uma das opções existentes para abusar da negligência humana que em seu momento presente pode ser a chave de entrada por cima de todas ferramentas e controles tecnológicos que serviriam de barreira.

" A engenharia social não prospera na suposição de que as pessoas são tolas, mas na percepção de que indivíduos podem ser facilmente manipulados a depositar confiança equivocada." (MITNICK; SIMON, 2003, p.16). Cabe a entender que o foco maior das tentativas de entrada, envolve-se no fato de que o humano é suscetível ao erro ou até mesmo a leve distraída que permitirá o ataque cibernético.

4 PHISHING, ENGENHARIA SOCIAL E OUTROS GOLPES

A Engenharia Social representa uma das maiores ameaças à segurança cibernética moderna, pois ataca o ponto mais vulnerável das organizações: o ser humano. Trata-se de uma técnica de manipulação psicológica usada por criminosos para enganar pessoas e levá-las a revelar informações confidenciais ou executar ações prejudiciais (Asper Tec., Cloudflare). Diferente dos ataques tradicionais, que exploram falhas em sistemas, a Engenharia Social explora falhas comportamentais, e basta o erro de um único funcionário para comprometer toda a rede corporativa (IBM). Com o avanço da tecnologia, especialmente o uso de Inteligência Artificial (IA), essas táticas se tornaram ainda mais sofisticadas, permitindo a criação de mensagens personalizadas e difíceis de detectar (Asper Tec.).

Entre as formas mais comuns de Engenharia Social está o *phishing*, em que mensagens falsas são usadas como “iscas” para induzir as vítimas a agirem impulsivamente (Venturus, IBM). Esse tipo de ataque evoluiu e deu origem a variações como *spear phishing*, *whaling*, e o *smishing*. O uso de IA ampliou ainda mais esses golpes, com o emprego de *deepfakes* e clonagem de voz para imitar pessoas reais, como CEOs e gestores, o que já causou prejuízos milionários em diversas organizações (Rede Líderes, ESR/RNP, MPMT).

O sucesso da Engenharia Social está diretamente ligado à manipulação emocional. Os golpistas exploram gatilhos psicológicos como medo, urgência, ganância, curiosidade e autoridade (IBM). A vítima, sob pressão emocional, tende a agir sem refletir, ignorando sinais de alerta, como URLs falsas ou erros de ortografia. Por isso, a defesa contra esse tipo de ameaça deve ir além da tecnologia, exigindo que as pessoas desenvolvam hábitos de verificação automáticos e pensamento crítico, especialmente em situações de alta pressão (IBM).

Os impactos de um ataque de Engenharia Social podem ser devastadores, afetando finanças, reputação e continuidade operacional. Para mitigar esses riscos, é essencial adotar uma “defesa em profundidade”, combinando tecnologia e conscientização humana (Rede Líderes, Addit). Entre as principais medidas estão a autenticação multifator (MFA), a implementação da arquitetura Zero Trust, a gestão rigorosa da confidencialidade e o uso de protocolos de verificação não verbal (Staysafeonline, IBCybersecurity, Serasa). No entanto, mesmo tecnologias avançadas, como o MFA, podem ser comprometidas se o usuário for manipulado a aprovar acessos indevidos — reforçando a necessidade de treinamento e vigilância (IBM).

O treinamento em segurança da informação é um pilar essencial na prevenção de ataques de Engenharia Social. Programas contínuos de conscientização, com simulações realistas de phishing e orientações sobre novas ameaças como *deepfakes* e *vishing*, reduzem drasticamente a vulnerabilidade humana (Proofpoint, Rede Líderes, ESR/RNP). Estudos mostram que empresas que investem em educação contínua conseguem reduzir em até 89% a suscetibilidade a ataques (Proofpoint). Além disso, o fortalecimento da cultura organizacional de segurança é fundamental: a proteção deve ser um valor compartilhado e incorporado ao cotidiano da empresa (IBCybersecurity, Engehall, Dataguide, Microsoft).

De outra perspectiva, a Engenharia Social é o “hacking humano”, uma forma de ataque que explora emoções como confiança, medo e urgência em vez de vulnerabilidades técnicas (Asper Tec., IBM). O combate eficaz exige tanto defesas tecnológicas robustas, quanto o fortalecimento da consciência e da cultura de segurança entre os colaboradores. Somente quando a segurança se torna parte da identidade organizacional é que cada funcionário passa a agir como a primeira linha de defesa contra ataques psicológicos e cibernéticos (Engehall, Rede Líderes).

5 QUANDO UM CLIQUE CUSTA MILHÕES

O estudo de caso a seguir, tem como foco abordar um crime cibernético cometido indiretamente ao Banco Central do Brasil, com foco em discorrer a que se referem às metodologias, métodos e conceitos, uso e fornecimento indevido de credenciais e brechas de segurança exploradas, ressalvando a importância de investimento em melhores sistemas de segurança, e manter uma equipe fidedigna acerca de tamanha responsabilidade a que se referem os sistemas financeiros, tão quanto quando estão ligados diretamente ao Banco Central, responsável pelo controle monetário brasileiro e da garantia pela estabilidade financeira do país.

O ataque ocorreu na madrugada de 28 de julho de 2025 a uma empresa responsável por intermediar transações pix entre o Banco Central e outras instituições, e consistiu em utilizar técnicas de engenharia social para coagir um funcionário da empresa a fornecer suas credenciais de acesso ao grupo criminoso, que realizou diversas transações via PIX, se estipula que o prejuízo gire em torno de R$400 milhões a R$800 milhões (TIINSIDE, 2025). É válido ressaltar que as práticas de engenharia social foram cruciais para que o ataque fosse bem-sucedido, visto que utilizam-se técnicas de manipulação para explorar a confiança de alguém (DIARIO DO POVO, 2025), como foi o caso anteriormente descrito, o funcionário fornece suas credenciais para o grupo criminosos após ser abordado pessoalmente por um deles, que ofereceu inicialmente um valor em dinheiro e resultou no desvio de uma quantidade milionária dentro do sistema (O GLOBO, 2025), os criminosos utilizaram celulares descartáveis para a comunicação com o funcionário.

O ocorrido trata-se de um ataque direto a cadeia de suprimentos (supply chain) não sendo possível prever e calcular os danos acarretados após uma invasão,

devido ao fato de terem comprometido o sistema de uma empresa intermediadora, fundamental para que os processos transacionais sejam bem-sucedidos. Os atacantes souberam economizar tempo utilizando a engenharia social, por consequência conseguiram também economizar dinheiro, mesmo após comprometer credenciais verdadeiras por meio de suborno (METRÓPOLES, 2025), não tiveram o trabalho de preocuparem-se em explorar brechas, aquisições de softwares ilegais que permitissem a invasão, gastos com equipamentos, ou até mesmo a necessidade de contratação de outra equipe especializada de criminosos(apesar de não saber-se ao certo o número de envolvidos) como parte complementar da quadrilha (crime organizado). Conseguiram ainda criar uma janela menor de detecção do ataque antes de concluí-lo, visto que, a partir do momento do ataque, tratou-se de um funcionário em horário de trabalho, utilizando credenciais verdadeiras e com autorização corporativa para realizar as transações, somente após 3 horas de ataque houve desconfiança das operações.

Partindo diretamente para um ataque ao Banco Central, o grupo teria de conhecer o sistema interno de segurança, mapeando as possíveis brechas para depois aproveitar-se delas, tal ação levaria muito tempo para preparo, além de correrem o risco de serem expostos, ou não possuírem fontes confiáveis para obter essas informações, abrindo espaço para sucessivas chances de falhar no ataque. Diante da gravidade do problema o crime equipara-se a uma doença, que ao infiltrar-se no sistema nervoso central, é capaz de não apenas comprometer o coração, mas também outros órgãos vitais, sendo muito mais viável burlar o sistema imunológico e infiltrar-se em uma única veia, ao invés de desenvolver-se lentamente direto a um órgão específico. A empresa vítima do ataque classifica-se como BaaS (Banking as a Service) e permite que fintechs, empresas, desenvolvedores e bancos operem serviços financeiros em suas plataformas com sua própria marca por meio de API´s (C6, 2025), estas possuem funcionalidades bancárias como transações, além de facilitarem operações, permitirem comunicação entre diferentes sistemas e softwares, e compartilhamento de dados de maneira padronizada e segura.

6 O CUSTO REAL DE UMA BRECHA DE CENTAVOS

No atual contexto corporativo a informação acaba virando um dos recursos mais valiosos dentro de uma empresa. E mesmo assim muitas pessoas subestimam os impactos financeiros e reputacionais causados por uma simples brecha de

segurança, como anexos maliciosos, pendrives infectados ou senhas fracas. Isso acaba desencadeando grandes prejuízos para empresa.

Novos estudos demonstram que os custos relacionados a incidentes cibernéticos não ficam presos somente a sistemas que foram comprometidos. Existem outras despesas como perda de dados sensíveis, paralisação das operações, ações judiciais, multas por não conformidade com legislações de proteção de dados como a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais) . Segundo o Relatório da IBM: Custo médio de uma violação de dados no Brasil atinge R$ 7,19 milhões, em 2025 o brasil indicou um crescimento no custo médio dos vazamentos de dados em comparação a seu ano anterior de 6,5% indo de 6,75 milhões para 7,19 milhões e em sua grande maioria está relacionada a negligência operacional ou a erros humanos.

Tendo isto como base, as empresas atuais devem buscar os pilares para a segurança da informação ele sendo confidencialidade, integridade e disponibilidade, os três pilares do modelo conhecido como Tríade CID pois este método além de lhe auxiliar nos acessos que as pessoas têm dentro da empresa também auxilia para identificar as informações que os invasores podem estar atrás e auxilia a blindar as mesmas contra ataques.

Portanto, compreender o custo real de uma brecha de segurança ajuda a entender que a prevenção é melhor que a remediação pois os investimentos em segurança podem ser considerados baixos se compararmos com os prejuízos que podem ser causados e não se limitam apenas ao financeiro, já que também afetam a reputação, confiabilidade da empresa e de tudo que ela representa.

7 TREINAMENTO E CULTURA DE SEGURANÇA: A PRIMEIRA LINHA DE DEFESA

Atualmente o maior problema das empresas na segurança de dados é o fator humano, segundo estudos realizados pela Mimecast (2025) aponta que 95% das violações de dados foram causadas por erro humano sejam elas causadas por desatenção, descumprimento de políticas internas ou falta de conhecimento.

Tendo isto como base só ressalta a importância de treinamentos e a cultura da segurança da informação como a primeira linha de defesa das organizações. Pois um funcionário bem instruído seria capaz de identificar tentativas de *phishing*,

engenharia social e entre outras. Mas em comparação um funcionário despreparado pode acabar se tornando o elo fraco de toda a rede de segurança de uma empresa, praticamente invalidando todo o investimento em tecnologias para a segurança das informações.

Para a redução desses casos é necessário algo além de treinamentos esporádicos e sim uma mudança na mentalidade organizacional, ou seja, que seja incorporada no dia a dia dos processos e decisões.

Os melhores exemplos para aplicação seria:

- Simulação de *phishing*: Envio de emails falsos de phishing para avaliar quais colaboradores estão sujeitos a cair em golpes e reforçar o aprendizado prático.
- Criação de canais de comunicação interna: Isto facilitaria a comunicação da empresa para relatar reportes de incidentes e de boas práticas de segurança
- Programa de capacitação contínua: Cursos ou palestra de segurança adaptados à realidade da empresa.
- Programa de recompensas: Fornecer recompensas ou feedbacks para os que realizam comportamentos corretos.

A empresa também tem que se adaptar criando um sistema de aprendizagem organizacional, no qual usa como base ocorridos anteriores para que possa se aperfeiçoar, pois do mesmo método que as tecnologias evoluem com o tempo os softwares e os métodos de quebrar a segurança das empresas também.

Logo, a tecnologia não é a primeira linha de defesa, mas sim as pessoas. Pois elas são o ponto inicial para a proteção digital e somente após aperfeiçoar isso se tem um ambiente realmente firmado para enfrentar os métodos de *phishing* e engenharia social, aumentando assim a segurança dentro da empresa.

8 MENSURAÇÃO DE RESULTADOS: INDICADORES PARA AVALIAR A CONSCIENTIZAÇÃO

O treinamento dos colaboradores é essencial, mas a mensuração de resultados em programas de conscientização de segurança é o que transforma atividades de treinamento em investimentos estratégicos com retorno demonstrável. Ao trabalhar com Indicadores-Chave de Desempenho (KPIs), as organizações conseguem traduzir esforços em dados tangíveis que comprovam a mudança de comportamento e a redução de riscos. Contudo, o excesso de dados pode levar à perda de foco, tornando-se fundamental identificar "as principais ferramentas de orientação na medição da segurança da informação" (HUMPERT-VRIELINK; VRIELINK, 2012, p. 49).

Dentre as métricas mais significativas, destacam-se os resultados de simulações de *phishing* - incluindo taxa de cliques, comunicação e reincidência - que avaliam diretamente a efetividade do treinamento e a mudança de comportamento. A taxa de conclusão dos treinamentos serve como indicador básico de adesão, enquanto métricas operacionais como Tempo Médio para Detectar (MTTD) e Responder (MTTR) a incidentes podem ser indiretamente impactadas por uma força de trabalho mais consciente.

Outro ponto importante é o alinhamento estratégico das métricas, pois "queremos que todos estejam alinhados, quais são as métricas da empresa, quais são as métricas cibernéticas, o que a TI está fazendo durante o processo, está melhorando ou dificultando as coisas, e ser capaz de identificar o que é prioridade para cada grupo" (HANCOCK; GEOFF, 2025, 28m43s).

Dessa forma, um programa de conscientização sustentado por uma mensuração bem estruturada deixa de ser uma despesa para se tornar a primeira linha de defesa, demonstrando concretamente que a organização está tratando o fator humano com a seriedade necessária e transformando cada usuário em um aliado ativo na proteção do negócio.

9 PLANO DE MITIGAÇÃO: TECNOLOGIA + PREPARO HUMANO

Após analisar o ocorrido mencionado no estudo de caso, confirma-se que a maior falha em um sistema financeiro é o fator humano, seja por erros, ações e decisões não pretendidas, ou violações, desvios intencionais de regras e procedimentos. É possível avaliar os riscos para implementar medidas de proteção para o sistema, a fim de proteger a cadeia de suprimentos, visto que, uma vez que o sistema financeiro deixa de ser composto somente por uma instituição, o fator segurança é expandido ainda mais, surgindo outras brechas de segurança, que devem ser protegidas pelas instituições parceiras. Existem normas e padrões que possibilitam orientar as empresas de maneira a que se enquadrem nos critérios e princípios primordiais de segurança cibernética, como no caso do Padrão de Segurança de Dados da Indústria de Cartões de Pagamento (PCI DSS 4.0), Instituto Nacional de Padrões e Tecnologia (NIST) e autenticação multifator (MFA), além de práticas como capacitações, treinamentos e especializações de funcionários e verificação de identidade.

O PCI DSS 4.0 é um documento normativo acerca de regras, metodologias e padrões de segurança que devem ser seguidos obrigatoriamente pelas instituições financeiras brasileiras, a fim de garantir um ambiente seguro aos clientes que utilizem cartões de crédito e débito para realizar transações. O principal objetivo é semelhante a que se referem a associação brasileira de normas técnicas (ABNT), porém destinadas ao setor de segurança financeira, no documento estão descritos os procedimentos que devem ser seguidos ao construir e manter uma rede e seus sistemas seguros, proteção de dados da conta, manter um programa de gestão de vulnerabilidade, implementação de medidas fortes de controle de acesso, entre outros.

Muitas empresas brasileiras adotam as normas e diretrizes do NIST, uma agência dos Estados Unidos que retrata diretrizes estruturadas em cinco funções principais para gerenciar e prevenir riscos de segurança cibernética: Identificar, detectar, responder e recuperar. Grandes empresas nacionais como Banco do Brasil, Bradesco e Microsoft Brasil recorrem ao NIST principalmente para alinharem-se às boas práticas internacionais de segurança e para melhorar a gestão de riscos cibernéticos. Embora as normas do NIST não sejam obrigatoriamente seguidas, elas

podem servir como referência de boas práticas de segurança.

Em tempos de constante evolução, inovações e conexão, as transações financeiras estão cada vez mais eficientes, práticas e fáceis, o pix é uma prova viva dessa afirmação, e dentro das instituições responsáveis pelo gerenciamento desses sistemas é importante manter-se uma equipe de tecnologia da informação (T.I) alinhada às práticas e estratégias da Gestão de Acesso Privilegiado (PAM), que consistem em práticas essenciais de segurança cibernética, concentrados no controle e monitoramento de acessos privilegiados em sistemas de T.I, proteger e monitorar contas com maior nível de acesso à dados sensíveis, juntamente com à Gestão de Acesso e Identidade (IAM), esta refere-se a um conjunto de políticas, processos e tecnologias voltados para controlar o acesso a dados e recursos digitais, a fim de prevenir fraudes, acessos não autorizados e vazamento de dados, para isso são utilizados o gerenciamento de identidade, controlando e administrando as credenciais dos usuários, permitindo um perfil único em um ambiente online seguro, já o gerenciamento de acesso determina quais as permissões que determinados usuários podem ter dentro do sistema, isso também inclui monitoramento de acesso a dispositivos desconhecidos, localização, horário e dispositivo conectado.

Por fim, entende-se que nenhum sistema está totalmente seguro, independente de qual ele seja, sempre haverá o risco de possíveis invasões e vazamento de dados, uma vez que as tecnologias e meios digitais estão em constante evolução, para manter uma instituição mais segura possível é necessário que a equipe como um todo trabalhe focada mutuamente nos processos de treinamentos, gestões e normativos, para que se desenvolva um ambiente online seguro e confiável.

10 CONCLUSÃO - TRANSFORMANDO USUÁRIOS EM ALIADOS DA SEGURANÇA

Por mais que organizações invistam fortunas em tecnologias de ponta, é a ação humana, no caso a falha dela, que continua abrindo portas para invasores. O caso do ataque ao sistema Pix, que foi citado anteriormente, com seus prejuízos astronômicos, nos lembra que firewalls e criptografia têm limites claros quando um funcionário, seja por ingenuidade ou pressão excessiva imposta pela empresa, se torna o ponto de falha. Como bem observaram especialistas na área, "as pessoas são o fator mais crítico na proteção da segurança cibernética, mas também são o elo

mais fraco do sistema" (PAN et al., 2012, p. 278). Essa constatação reforça que a segurança não fica completa sem o fator humano.

No entanto, implantar programas de treinamento é apenas o começo, o desafio está em mantê-los de maneira eficiente e melhorando durante o fluxo. A mensuração contínua por meio de indicadores práticos como taxas de clique em *phishing* e tempo de resposta a incidentes, transforma o esforço de conscientização em um ciclo de aprendizado. Esses dados permitem às empresas se adaptarem. Dessa forma, a segurança deixa de ser algo repetitivo e maçante, adaptando-se tanto às novas ameaças quanto às necessidades reais das equipes.

Assim, concluímos que transformar usuários em aliados pode ser um gasto no começo, mas se mostra como o investimento mais inteligente que uma organização pode fazer. Essa jornada exige paciência e persistência, mas o retorno é perceptível, resulta em um ambiente onde tecnologia e pessoas se reforçam mutuamente. Quando cada colaborador entende seu papel na defesa do todo, a "brecha de centavos" se fecha quando todos os fragmentos estiverem em seu devido lugar.

REFERÊNCIAS

ADDIT. **Os pilares fundamentais da segurança da informação.** Disponível em: https://addit.com.br/pilares-da-seguranca-da-informacao/. Acesso em: 30 set. 2025.

ALCOFORADO, Acilégna Cristina Duarte Guedes; RIBEIRO, Emerson da Cruz; CUNHA, Jacqueline de Araújo. **Condutas do fator humano: alicerce da segurança da informação.** MOCI – Revista de Ciência da Informação, Belo Horizonte, v. 2, n. 2, p. 1–15, 2021. Disponível em: https://periodicos.ufmg.br/index.php/moci/article/view/17534/14317. Acesso em: 8 out. 2025.

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

ASPER TEC. **Engenharia Social – O elo mais fraco na cibersegurança**. Disponível em: https://blog.asper.tec.br/engenharia-social-ciberseguranca/. Acesso em: 30 set. 2025.

BRASIL. **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 (Lei Geral de Proteção de Dados Pessoais – LGPD).** *Diário Oficial da União*, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm Acesso em 29. Set.2025.

C6. **Banking as a Service: o que é e como funciona?** Disponível em: https://www.c6bank.com.br/blog/banking-as-a-service. Acesso em 12. Set.2025.

CLOUDFLARE. **Como funcionam os ataques de engenharia social?**. Disponível em: https://www.cloudflare.com/pt-br/learning/security/threats/social-engineering-attack/. Acesso em: 30 set. 2025.

DATAGUIDE. **Introdução à análise de maturidade em segurança da informação.** Disponível em: https://dataguide.com.br/introducao-a-analise-de-maturidade-em-seguranca-da-informacao/. Acesso em: 30 set. 2025.

DIARIO DO POVO. **Funcionário da C&M Software é desligado após golpe milionário com credenciais roubadas.** Disponível em: https://diario.dopovo.com.br/2025/07/04/funcionario-da-cm-software-e-desligado-apos-golpe-milionario-com-credenciais-roubadas/#google_vignette. Acesso em: 12 set. 2025.

DHILLON, G. **Realizing benefits on an information security program. Business Process Management Journal**. Business Process Management Journal, 10 (3), 2004. Páginas 260-261.

ESCOLA SUPERIOR DE REDES (RNP). **6 melhores práticas de segurança da informação para empresas.** Disponível em: https://esr.rnp.br/seguranca/melhores-praticas-de-seguranca-da-informacao/. Acesso em: 30 set. 2025.

ENGEHALL. **Nível de maturidade da cultura de segurança: Saiba avaliar.** Disponível em: https://engehall.com.br/maturidade-da-cultura-de-seguranca/. Acesso em: 30 set. 2025.

G1. **Ataque hacker ao sistema financeiro: BMP perdeu, sozinha, R$ 541 milhões, outras instituições também foram afetadas.** Disponível em: https://g1.globo.com/economia/noticia/2025/07/04/ataque-hacker-recursos-desviados.ghtml. Acesso em 27. Set 2025.

HANCOCK; Geoff. **Cybersecurity Metrics & KPIs CISOs Use To Prove Value.** YouTube, 2025. Disponível em https://www.youtube.com/watch?v=XJE_KojgFIY . Acesso em 02 de Outubro de 2025.

IBM. ***Phishing*.** Disponível em: https://www.ibm.com/br-pt/think/topics/phishing. Acesso em: 30 set. 2025.

IBM. ***Relatório da IBM: Custo médio de uma violação de dados no Brasil atinge R$7,19milhões*** Disponível em: https://brasil.newsroom.ibm.com/2025-07-30-Relatorio-da-IBM-Custo-medio-de-uma violacao-de-dados-no-Brasil-atinge-R-7,19-milhoes. Acesso em: 27 Setembro. 2025.

IBM. ***Social Engineering*.** Disponível em: https://www.ibm.com/br-pt/think/topics/social-engineering. Acesso em: 30 set. 2025.

Kahneman, D. & Knetsch, J. & Thaler, R. (1990). "Experimental tests effect and the Coase theorem." Journal of Political Economy 98: Páginas 1325-1348.

KAHNEMAN, D. & KNETSCH, J. & THALER, R. (1991). **"Anomalies: the endowment effect, loss aversion, and status quo bias."** Journal of Economic Perspecbtives 5(1): Páginas 193-206.

HUMPERT-VRIELINK, Frederik; VRIELINK, Nina. **A modern approach in information security measurement.** In: _____. (Ed.). Securing electronic business processes. Wiesbaden: Springer Fachmedien, 2012. Páginas 48-53.

MANN, Ian. **Engenharia social.** São Paulo: Edgard Blücher, 2003.

METRÓPOLIS. **Ataque hacker que drenou R$ 541 milhões via Pix durou 5h na madrugada.** Disponível em: https://www.metropoles.com/sao-paulo/ataque-hacker-que-drenou-r-541-milhoes-via pix-durou-5h-na-madrugada. Acesso em 27. Set 2025

MICROHARD. **Deepfake e Engenharia Social: A Ameaça Silenciosa que Pode Derrubar sua Empresa.** Disponível em: https://microhard.com.br/deepfake-e-engenharia-social-a-ameaca-silenciosa-que-po de-derrubar-sua-empresa/. Acesso em: 30 set. 2025.

MINISTÉRIO PÚBLICO DO ESTADO DE MATO GROSSO (MPMT). **Estudo mostra que 70% das empresas preveem alto impacto de ataques com deepfake.** Disponível em: https://www.mpmt.mp.br/conteudo/1217/145271/estudo-mostra-que-70-das-empresas-preveem-alto-impacto-de-ataques-com-deepfake. Acesso em: 30 set. 2025.

MIMECAST. ***The State of Human Risk 2025.*** Disponível em: https://www.mimecast.com/resources/ebooks/state-of-human-risk-2025/. Acesso em: 07 out. 2025.

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar: ataques de hackers: controlando o fator humano na segurança da informação.** São Paulo: Pearson Universidades, 2003.

NIST. **Digital identity guidelines.** Disponível em: https://pages.nist.gov/800-63-3/sp800-63b.html. Acesso em: 27. Set 2025

O GLOBO. **Engenharia social, 'insider' e venda de senha: entenda o desvio milionário do sistema do Pix.** Disponível em: https://oglobo.globo.com/economia/financas/noticia/2025/07/04/engenharia-social-insider-e-venda-de-senha-entenda-o-desvio-milionario-do-sistema-do-pix.ghtml. Acesso em: 12 set. 2025.

PAN, Shin Ming et al. **Cybersecurity: Public Sector Threats and Responses.** Boca Raton: CRC Press, 2012. Disponível em: https://library.oapen.org/bitstream/handle/20.500.12657/40114/1/9781439846636.pdf. Acesso em: 3 de outubro de 2025.

PCI. **Padrão de segurança de dados.** Disponível em: https://listings.pcisecuritystandards.org/documents/PCI-DSS-v4_0-PT.pdf. Acesso em 12. Set 2025

PFLEEGER, Charles P.; PFLEEGER, Shari Lawrence. **Security in Computing.** 5. ed. Upper Saddle River: Prentice Hall, 2012.

PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO DE JANEIRO — PUC-RIO. **Engenharia social.** Especialização CCEC — PUC-RIO, s.d. Disponível em: https://especializacao.ccec.puc-rio.br/blog/engenharia-social. Acesso em: 07 out. 2025.

PROOFPOINT. **Treinamento de segurança da informação - Security Awareness Training.** Disponível em: https://www.proofpoint.com/br/threat-reference/security-awareness-training. Acesso em: 30 set. 2025.

REDE LÍDERES. ***Como proteger empresas contra a engenharia social.*** Disponível em: https://redelideres.com/2025/02/06/como-proteger-empresas-contra-a-engenharia-social/. Acesso em: 30 set. 2025.

SERASA. ***Vishing, smishing ou phising: entenda a diferença*****.** Disponível em: https://www.serasa.com.br/premium/blog/vishing-smishing-ou-phishing-qual-a-diferenca/. Acesso em: 30 set. 2025.

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

TIINSIDE. **Incidente com a C&M e o PIX: lições para construir uma Supply Chain segura.** Disponível em: https://tiinside.com.br/15/07/2025/incidente-com-a-cm-e-o-pix-licoes-para-construir-uma-supply-chain-segura/. Acesso em: 12 set.2025.

WEIGERT, Alexsander; CASTILHO JÚNIOR, Gelásio Onofre de. **Utilização de firewall em aplicação de segurança e ferramentas gerenciais. Trabalho de Conclusão de Curso (Graduação)** — Universidade Tecnológica Federal do Paraná, UTFPR, 2017. Disponível em: https://riut.utfpr.edu.br/jspui/bitstream/1/9706/1/CT_COTEL_2017_1_1.pdf. Acesso em: 9 out. 2025.