REVISTA JURÍDICA DA FA7 FA7 LAW REVIEW
PERIÓDICO CIENTÍFICO DO PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO DA UNI7

Submissão #1843
Submetido em: 22/10/2025
Aprovado em: 31/03/2026

Segurança digital e a resiliência cibernética nacional

Emerson Wendt
Universidade La Salle – Canoas/RS
emersonwendt@gmail.com

Candido Heleno Grasel
PagoNXT
candido.grasel@gmail.com

Resumo

A resiliência cibernética é essencial para a segurança nacional, pois um país vulnerável a ataques cibernéticos pode sofrer sérias consequências econômicas, políticas e sociais. Nesse contexto, esta pesquisa investiga como a percepção de segurança digital dos brasileiros afeta a resiliência cibernética nacional. O estudo concentra-se em compreender como aspectos comportamentais, sociais e psicológicos influenciam essa percepção e como práticas de conscientização e educação em segurança cibernética podem ser aprimoradas. A hipótese central é que a percepção de segurança digital está diretamente ligada a esses aspectos, o que se reflete em hábitos online seguros ou inseguros e, consequentemente, afeta a resiliência cibernética do país. O objetivo é identificar os fatores que influenciam a percepção de segurança digital e propor estratégias para elevar a maturidade da segurança cibernética nacional. Além disso, a pesquisa contribui para o entendimento do papel das percepções individuais na segurança cibernética de um país, destacando a importância de abordagens educacionais e de conscientização específicas. A metodologia adotada é a pesquisa bibliográfica, que permite a análise e síntese de conhecimentos já existentes sobre o tema.

Palavras-chave

Digital. Infraestrutura. Resiliência. Segurança. Sociedade.

1. Introdução

O dicionário brasileiro da língua portuguesa define resiliência em um dos seus significados como “capacidade de rápida adaptação ou recuperação”. Quando trazemos este contexto para o ambiente cibernético, podemos definir ciber resiliência como sendo a habilidade de “permanecer de pé” mesmo apesar de sucessivos ciberataques, recuperando-se com rapidez e mantendo as coisas funcionando em seu estado normal de operação. A necessidade de uma sociedade ser ciberneticamente resiliente fica mais evidente tendo em vista a dependência do ecossistema digital para seu pleno funcionamento, inclusive em infraestruturas críticas.

A Política Nacional de Segurança de Infraestruturas Críticas – PNSIC, conforme Decreto Nº 11.200, de 15 de setembro de 2022, define infraestruturas críticas como “[...] instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial,

Submissão #1843
Submetido em: 22/10/2025
Aprovado em: 31/03/2026

provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade", dentre as quais podem ser citadas a título de exemplo as áreas de águas e energia.

Em vista de estas infraestruturas estarem cada vez mais interconectadas a rede mundial de computadores, objetivando assim facilitar a gerência e manutenção de dispositivos e controladores que compõem seus sistemas, é importante ressaltar que esta interconexão aumenta também a superfície de ataque a estas infraestruturas através de vulnerabilidades exploradas em Sistemas de Controle Industrial – dado que estes ambientes em sua maioria são sistemas legados[1] – bem como em ataques direcionados a funcionários de entidades que englobam estes setores.

Embora avanços legislativos a nível nacional já tenham sido feitos com intuito de aumentar o conhecimento da sociedade brasileira sobre as novas tecnologias digitais, a exemplo da Lei Nº 15.533, de 11 de Janeiro de 2023, que institui a Política Nacional de Educação Digital, a qual tem por foco promover a inclusão digital e o uso das tecnologias de informação na educação, são muitos os percalços a serem superados.

Semanalmente a mídia noticia casos de aplicação de golpes praticados por meios eletrônicos, em especial através de dispositivos smartphones. Estes tipos de fraudes têm como público-alvo majoritário as populações mais carentes de conhecimento digital. Do envio de e-mails fraudulentos, mensagens SMS forjadas para direcionar a vítima para conteúdo malicioso, até centrais de atendimento do crime contando com diversos "empregados" e desenvolvidas com intuito de induzir as vítimas a fornecer suas informações bancárias, a criatividade dos golpistas para o crime só aumenta ano após ano.

Com a falta do adequado conhecimento acerca dos riscos inseridos na utilização de sistemas de informação, o comportamento humano tem especial relevância para aumentar ou enfraquecer a resiliência cibernética do país, uma vez que os cidadãos em sua vida particular e como trabalhadores são cada vez mais usuários de sistemas informáticos para executar suas atividades e estando assim sujeitos a diversos tipos de ataques por parte de criminosos que querem obter vantagem ilícita; nem que para isto seja necessário interromper o abastecimento de água de uma determinada

[1] Sistema legado: São sistemas em obsolescência que estão em uso dentro de uma companhia por muitos anos. Em resumo, são sistemas que não possuem mais suporte de seu fabricante.

Submissão #1843
Submetido em: 22/10/2025
Aprovado em: 31/03/2026

localidade, paralisar a distribuição de energia ou eliminar as reservas financeiras de uma família.

Buscar-se-á neste artigo encontrar respostas para o problema de pesquisa temático: como a percepção de segurança digital dos brasileiros pode ser afetada por aspectos comportamentais, sociais e psicológicos, e como estes podem potencializar – ou enfraquecer - as defesas cibernéticas do país. Para tanto, buscar-se-á confirmar a hipótese de que estes aspectos comportamentais, sociais e psicológicos podem afetar diretamente a ciber resiliência brasileira, fazendo isso através de uma revisão bibliográfica que abrange diferentes perspectivas da segurança da informação.

Assim, o trabalho foi dividido em três tópicos principais, sendo que o primeiro abordará a dualidade da tecnologia, que, embora fundamental para a sociedade moderna, é cada vez mais empregada como ferramenta em conflitos e atividades ilícitas. Serão explorados exemplos de ciberataques a infraestruturas críticas e empresas, demonstrando o impacto econômico e social. Além disso, o tópico detalha a evolução das fraudes eletrônicas, evidenciando como a tecnologia facilita a ação de criminosos e a necessidade de medidas de segurança robustas.

Já o segundo tópico aprofundará a discussão sobre o elemento humano na segurança digital, analisando como vulnerabilidades comportamentais, sociais e psicológicas são exploradas por agentes mal-intencionados. Será destacada a engenharia social como uma tática eficaz para manipular indivíduos e obter acesso a informações confidenciais. O tópico também buscará comparar o ambiente físico com o ciberespaço, sublinhando a importância da percepção de risco e do comportamento online para a resiliência cibernética, e a necessidade de programas de conscientização e educação.

No terceiro e último tópico, ressaltar-se-á o papel insubstituível do ser humano como a linha final de defesa contra ameaças cibernéticas. Serão examinadas as colaborações entre os setores público e privado, bem como a contribuição de empresas e organizações sem fins lucrativos na construção de um ecossistema de segurança cibernética robusto. Adicionalmente, o tópico discutirá a legislação vigente e a urgência de seu aprimoramento para garantir a responsabilização dos criminosos e a proteção dos cidadãos, enfatizando que a segurança digital é uma responsabilidade coletiva que exige a participação de todos os segmentos da sociedade.

Serão, ao final, fornecidas sugestões que contribuam para um aumento da maturidade de segurança digital no Brasil.

Submissão #1843
Submetido em: 22/10/2025
Aprovado em: 31/03/2026

2. Tecnologia como arma

Este capítulo mostrará como a tecnologia tem sido utilizada como certo tipo de arma atualmente, e que quando usada para o mal, pode acabar com a vida de pessoas ou até nações inteiras. Através deste tópico mostrar-se-á a relevância do problema de pesquisa no atual estado de coisas, uma vez que os ataques cibernéticos anualmente fazem milhares de vítimas, sejam através de ataques a infraestruturas críticas, ou até mesmo em ataques mais quotidianos, como no caso de fraudes eletrônicas.

2.1. De guerra

Em um ataque relativamente recente a Norsk Hydro - uma empresa de energia sediada na Noruega – o grupo de criminosos utilizou-se de e-mails de phishing cuidadosamente direcionados a funcionários desta organização, para assim entregar software malicioso, instalar-se nos sistemas da empresa e posteriormente criptografar os dados presentes nestes sistemas, paralisando as operações em cerca de 40 países em que esta empresa está sediada e causando um impacto de cerca de 71 milhões de dólares. Este ocorrido ilustra o potencial devastador de um ataque originado com base na exploração de fragilidades do ser humano, através de engenharia social combinada ao uso da tecnologia.

Dimaggio (2012, p.80) analisando o ciberataque à empresa do ramo de combustíveis Colonial Pipeline, ocorrido em 2021, e que resultou na paralisação da planta e consequentemente na distribuição de combustível para metade da Costa Leste dos Estados Unidos, conclui que governos (neste caso a Rússia) estão contratando ciber criminosos para realizarem suas atividades de ataque a infraestruturas críticas de nações inimigas, assim não sendo diretamente responsabilizados e evitando sanções internacionais.

No relatório anual OT[2] Cybersecurity: The 2023 Year In Review a empresa Dragos (2024, p.8), especializada em proteção de Sistemas de Controle Industriais, relata um aumento de 50% nos ataques observados a sistemas industriais em comparação com o ano anterior, tendo atingido cerca de 638 indústrias em 33 setores distintos, contabilizando 70% de todos os ataques por Ransomware no mesmo período.

O mesmo relatório ressalta a utilização destes softwares maliciosos como verdadeiras armas de guerra em conflitos globais, como por exemplo entre Ucrânia-Rússia e Israel-Hamas. Em especial o setor de energia é o mais afetado por estes

[2] OT: Acrônimo em inglês para Operational Technology. Refere-se ao hardware e software usado para monitorar e controlar dispositivos físicos, processos e eventos em sistemas industriais.

Submissão #1843
Submetido em: 22/10/2025
Aprovado em: 31/03/2026

ataques, os quais resultaram em impactos no fornecimento de serviços essenciais aos cidadãos visto que a maioria das necessidades básicas dependem de eletricidade para poderem ser atendidas. Em 2022 um ataque físico contra território ucraniano procedeu um anterior ciber ataque às linhas de transmissão de energia elétrica deste mesmo país, conforme exposto por Greenberg (2023).

Dado que ataques cibernéticos comparados a ataques cinéticos, onde necessariamente demandam o tipo de alguma força militar atacando por terra, água ou ar, representam um risco extremamente menor para os países atacantes, explica-se então a utilização cada vez mais constante de verdadeiros exércitos digitais empregados por Estados para submeter nações inimigas ao custo de zero baixas humanas e nenhuma pólvora.

2.2. Nas fraudes eletrônicas

Tudo que produzimos ou compramos, custa mais porque algum tipo de segurança é necessário para entregá-lo. Custos com proteção de segredos industriais através de sistemas de proteção física e lógica, contra roubo durante a logística no transporte de produtos, várias etapas do processo produtivo de um produto levam em conta os gastos com segurança na hora de comercializá-lo ao consumidor final. Como comenta Schneier (2010, p.985) “Security isn’t just a tax on the honest, it’s a very expensive tax on the honest. If all men were angels, just think of the savings!”[3]. Quem acaba pagando esta conta, é quem vive dentro da legalidade.

O Fórum Brasileiro de Segurança Pública (2023, p. 15) relata que no Brasil em 2022 foram aplicados cerca de 208 golpes por meio eletrônico por hora, totalizando 200.322 registros de fraude eletrônica, um aumento de 326,3% tomando como data base 2018. Estes números demonstram que o delinquente comum também vê os sistemas informáticos como uma forma de reduzir os riscos atrelados às suas atividades ilícitas. Se no passado era necessário um infrator possuir algum tipo de arma e ter que abordar sua vítima, correndo assim o risco de ser contido pela própria vítima ou pelos agentes da lei, atualmente as desvantagens dos crimes praticados por meio eletrônico são mínimas para os infratores.

A respeito de fraudes eletrônicas, a Lei nº 14.155 de 2021 alterou o Decreto-Lei nº 2.848, de 1940 (Código Penal) nos artigos:

[3] A segurança não é apenas um imposto sobre os honestos, é um imposto muito caro sobre os honestos. Se todos os homens fossem anjos, pense nas economias! (Tradução nossa).

Submissão #1843
Submetido em: 22/10/2025
Aprovado em: 31/03/2026

> *Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:*
> *Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.*
> *[...]*
> *Art. 171[...]*
> *Fraude eletrônica*
> *§ 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo [...].*

Wendt (2023, p.163-167) aponta em sua pesquisa, através do relato de agentes da lei, que apesar dos incrementos no Código Penal supracitados, os quais teriam por objetivo frear o aumento dos casos de fraudes envolvendo meios digitais, não estão sendo efetivos pois 'mesmo responsabilizando os autores, mesmo presos, continuam cometendo o crime, até de dentro do presídio' e a 'pena (para o crime) de fraude eletrônica é muito pequena'".

Devido a uma soma de fatores, que passa pelo modesto investimento público em ferramental para os agentes da lei poderem investigar efetivamente estes casos, da cooperação das plataformas de conteúdo que nem sempre apresenta retorno satisfatório ou em tempo adequado e uma legislação nem sempre muito clara com relação a estes tipos de crimes no que tange a aplicabilidade de punições dos infratores, as infrações continuam a crescer e multiplicar-se.

Atualmente – e possivelmente em épocas vindouras também - não há sistemas 100% seguros, nem mecanismos de defesa – como por exemplo antivírus – e proteção a fraudes que vão ser eficazes em todas as situações. Portanto os delinquentes utilizam a tecnologia como meio de aplicação das fraudes, mas sempre aliada a técnicas de engenharia social para aumentar suas chances de sucesso.

3. Explorando fragilidades humanas

Este capítulo visa trazer clareza sobre como o comportamento humano funciona, e acerca de que se hábitos que as pessoas em geral cultivam podem ser aproveitados por atores mal-intencionados para realizar a aplicação de fraudes e ataques com sucesso.

Submissão #1843
Submetido em: 22/10/2025
Aprovado em: 31/03/2026

Revisando obras que tratam da relação entre psicologia e o mundo digital, e relatos de pesquisadores em cibersegurança, buscar-se-á identificar se há elementos comportamentais e psicológicos humanos que culminem em hábitos digitais inseguros, e o reflexo que isto pode ter em âmbito geral a nível nacional caso grande parcela da população faça parte desta realidade.

3.1. Engenharia social

Conforme mencionado por Mitnick (2002, p.3):

> *As developers invent continually better security technologies, making it increasingly difficult to exploit technical vulnerabilities, attackers will turn more and more to exploiting the human element. Cracking the human firewall is often easy, requires no investment beyond the cost of a phone call, and involves minimal risk.*[4]

Portanto, em virtude do baixo investimento e da alta chance de retorno, a utilização de engenharia social na aplicação de fraudes eletrônicas é bastante comum.

Hadnagy (2018, p.556) define engenharia social como "[...] any act that influences a person to take an action that may or may not be in his or her interests"[5]. Para influenciar a vítima a tomar a ação desejada, o engenheiro social se vale de gatilhos emocionais, princípios psicológicos e de conhecimento sobre como funciona a constituição do cérebro humano.

Kosfeld (2015, p. 673) cita que a oxitocina, hormônio importante no comportamento social e associada a sentimentos de empatia é liberada na corrente sanguínea quando confiamos em alguém – não necessariamente quando confiamos, mas quando sentimos que alguém nos deu confiança. Uma vez que este hormônio é liberado, a pessoa sente-se mais propensa a atender as solicitações que venham de seu interlocutor. Um engenheiro social com intenções maliciosas pode se valer deste fato para induzir a vítima a cair em uma fraude, ou a fornecer informações que em situações normais não forneceria. Faz isto por proporcionar à vítima situações que propiciem a

[4] À medida que os desenvolvedores inventam tecnologias de segurança cada vez melhores, tornando cada vez mais difícil a exploração de vulnerabilidades técnicas, os invasores se voltarão cada vez mais para a exploração do elemento humano. A quebra do firewall humano geralmente é fácil, não requer nenhum investimento além do custo de uma ligação telefônica e envolve um risco mínimo. (Tradução nossa).
[5] Qualquer ato que influencie uma pessoa a tomar uma ação que pode ou não ser do seu interesse. (Tradução nossa).

Submissão #1843
Submetido em: 22/10/2025
Aprovado em: 31/03/2026

liberação deste hormônio, em geral por afagar o ego dela ou por se fazer parecer alguém de seu círculo social.

Mitnick (2002, p.7) ainda comenta que "In most cases, successful social engineers have strong people skills. They're charming, polite, and easy to like – social traits needed to establishing rapid rapport and trust[6] [...]", sendo neste caso a confiança um fator chave para o sucesso de um ataque bem sucedido.

Schneier (2010, p.5222) sobre a confiança, analisa que a sociedade humana como a conhecemos foi desenvolvida com base nesta, e que é impensável pararmos para refletir racionalmente acerca de toda e qualquer decisão que tomamos no dia a dia. Algumas destas decisões são baseadas em nossa genética, desenvolvida para funcionar de tal forma desde o início dos tempos, e tendemos a julgar desconhecidos como sendo moralmente aceitáveis, ou ao contrário a sociedade não funcionaria de forma adequada (por exemplo, pagamos nossos impostos ao governo por acreditar que o valor será investido nos melhores interesses da sociedade como um todo). Podemos aqui entender o porquê de ser difícil para algumas vítimas julgarem com mais cautela alguns tipos de 'iscas' elaboradas para que caiam em fraudes, pois consideram o desconhecido como sendo moralmente bom e dotado de boas intenções, preconcebendo-o como confiável.

Um engenheiro social que quer ser efetivo se vale de preparação para ter mais chances de sucesso. Hadnagy (2018, p. 4901) desenvolveu um modelo chamado de Pirâmide da Engenharia Social, onde a base desta pirâmide envolve a coleta de informações a respeito do alvo. Pensemos por um minuto na quantidade de informações que as pessoas diariamente postam em suas redes sociais de forma pública, a respeito de sua vida particular: família, casa, viagens, animais de estimação etc. O campo de coleta é vasto, e a própria vítima na maioria dos casos fornece todos os insumos para o engenheiro social planejar seu pretexto, próxima fase de um ataque, a qual pode ser exemplificado por um fraudador se passando pelo gerente do banco da vítima e oferecendo vantagens, ou informando que uma transação deve ser refeita e direcionando a vítima para uma conta de propriedade do criminoso.

Em geral conforme diz Schneier (2012, p. 4913):

> *[...] defectors are quicker to use technological innovations. Society has to implement any new security technology as a group, which implies*

[6] Na maioria dos casos, os engenheiros sociais bem-sucedidos têm fortes habilidades pessoais. Eles são charmosos, educados e fáceis de se gostar - características sociais necessárias para estabelecer um rápido relacionamento e confiança. (Tradução nossa).

Submissão #1843
Submetido em: 22/10/2025
Aprovado em: 31/03/2026

> *agreement and coordination and – in some instances – a lengthy and bureaucratic procurement process .[...] For example, its easier for a bank robber to use his new motorcar as a getaway vehicle than it is for the police department to decide it needs one, get the budget to buy one, choose which one to buy, buy it, and then develop training and policies for it.*[7]

Desta forma, estando sempre informados acerca de como funcionam as novas tecnologias, os criminosos estudam como podem tirar proveito de falhas sem que as pessoas comuns se apercebam, e compartilham estas informações com outros grupos de criminosos, nos quais na maioria dos casos têm sucesso antes que as defesas da sociedade civil possam se organizar e proteger de alguma forma a população em geral.

Em vista dos números apresentados anteriormente acerca de fraudes eletrônicas, é possível entender o que infere Schneier (2010, p. 4659) falando sobre crimes cibernéticos ao dizer que "[...] it's pedestrian, common, slowly evolving, affecting others, increasingly familiar, and [...] well-understood. So, it makes sense that we understate the risks and underfund security"[8]. É mais provável que ocorram investimentos em segurança se forem oriundos de eventos como por exemplo um ataque terrorista, do que crimes quotidianos os quais não tem tantos elementos que exagerem o risco e com isso façam que atitudes sejam tomadas de forma mais rápida.

Além da exploração das fraquezas do ser humano através de engenharia social, há outro aspecto que devemos considerar acerca do porquê os ataques cibernéticos têm sido bem-sucedidos.

3.2. Mundo real x Ciberespaço

Aiken (2010, p.10) dá indicativos interessantes acerca do motivo de as pessoas não se aperceberem das ameaças quando adentram o universo on-line:

> *But many people deny the awareness that they've entered a new environment when they go online, so they remain ignorant – and are*

[7] Os criminosos são mais rápidos para usar as inovações tecnológicas. A sociedade precisa implementar qualquer nova tecnologia de segurança como um grupo, o que implica acordo e coordenação e, em alguns casos, um processo de aquisição demorado e burocrático.[...] Por exemplo, é mais fácil para um ladrão de banco usar seu novo carro como veículo de fuga do que para o departamento de polícia decidir que precisa de um, obter o orçamento para comprá-lo, escolher qual comprar, comprá-lo e, em seguida, desenvolver treinamento e políticas para ele. (Tradução nossa).

[8] É trivial, comum, evolui lentamente, afeta outras pessoas, é cada vez mais familiar e [...] bem compreendido. Portanto, faz sentido subestimarmos os riscos e subfinanciarmos a segurança. (Tradução nossa).

Submissão #1843
Submetido em: 22/10/2025
Aprovado em: 31/03/2026

> *fooled by their sense that nothing has changed. They are sitting in their own homes, surrounded by familiar objects, after all, and their bodies are resting in the cushions of familiar chairs and sofas. In their minds, they have not "gone" anywhere. But the conditions and qualities of the online environment are different from real life. That is why our instincts, which were honed for the real world, fail us in cyberspace.*[9]

Dificilmente entraríamos em um bairro sabidamente perigoso a noite, sem ter muito conhecimento de quais são as entradas e saídas deste e desacompanhados. Atualmente a maioria das pessoas possui ao menos um dispositivo conectado a internet, não necessitando ir a um cibercafé, ou a um espaço público para ter acesso a suas redes sociais, e-mails e notícias. Este convívio se dá a partir do conforto de seus lares, e isto faz com que esta sensação de não estar indo a lugar algum, leve a desconsiderar que a internet pode ser exatamente esta mesma vizinhança perigosa.

Conforme comenta Aiken (2010, p.21) "[...] in the absence of real-world cues and other subtle pieces of information – facial expressions, body language, physical spaces – we aren't able to make fully informed decisions"[10]. Os engenheiros sociais se valendo deste fato a seu favor e por poderem estar anônimos sob de um perfil falso, agora tem mais chances de sucesso por não necessitarem estar frente a frente com a vítima, diminuindo até mesmo possíveis sentimentos de culpa devido a esta mesma distância física. Se antes nas guerras era necessário estar frente a frente com o inimigo e olhá-lo nos olhos antes de abatê-lo, atualmente devido a tecnologia, sobretudo a internet, tornou alcançável a pessoas com pouco conhecimento, porém dotados de má intenção, prejudicar o seu próximo.

Some-se a isto o fato de que as vítimas perdem as suas inibições pelo fato de pensarem estar em anonimato completo e assim não suscetíveis a qualquer tipo de impacto e não serem alvo de algum tipo de fraude. Para alguns, estar no ambiente online tem o mesmo efeito que o álcool produz, aumentando a sua impulsividade e afetando o julgamento acerca dos fatos. Ofertas tentadoras em banners de sites duvidosos, promessas de lucro rápido através da realização tarefas online, várias são as tentativas

[9] Mas muitas pessoas negam o fato de que entraram em um novo ambiente quando estão online, então permanecem ignorantes – e são enganados pelo seu falso senso que nada mudou. Estão sentadas em suas próprias casas, rodeadas por objetos familiares, e seus corpos descansando nos assentos familiares de cadeiras e sofás. Nas suas mentes eles não "foram" a lugar algum. Mas as condições e qualidades do ambiente online são diferentes da vida real. Este é o motivo de nossos instintos, os quais foram concebidos para o mundo real, nos falharem no ciberespaço. (Tradução nossa).
[10] Na ausência de evidências do mundo real e de outras informações sutis (expressões faciais, linguagem corporal, espaços físicos), não conseguimos tomar decisões totalmente informadas. (Tradução nossa).

Submissão #1843
Submetido em: 22/10/2025
Aprovado em: 31/03/2026

dos fraudadores para aumentar as suas vítimas através da impulsividade humana através da vontade das vítimas de 'tirar vantagem' em alguma situação.

Com a crescente adoção de modelos de inteligência artificial, a distinção entre mundo real e digital está ficando cada vez mais tênue. Os golpistas se aproveitando de tecnologias como deep fake tem cada vez mais criado fraudes elaboradas, como no caso de um ataque direcionado a um executivo de uma multinacional do setor financeiro. Os golpistas se passando pelo Diretor Financeiro da empresa durante uma chamada de vídeo conferência, desviaram com o apoio do executivo enganado, cerca de 25 milhões de dólares das contas da multinacional (CNN, 2024).

Vemos assim que o comportamento humano tem um papel fundamental tratando-se de segurança digital. Mas há casos em que mesmo tendo certo nível de conhecimento acerca das ameaças do mundo digital, as pessoas ainda são impactadas. O que pode estar envolvido neste caso?

3.3. Conhecimento x Intenção x Comportamento

O evangelista em cibersegurança Carpenter P. (2018, p.22) argumenta que "[...] Just because [...] people are aware of something doesn't mean that they will care. [...] Even if they care and intend to do the right thing [...] contexts can interfere with [...] behavior [...]"[11]. Assim sendo, mesmo nos casos em que o indivíduo tenha conhecimento acerca dos golpes praticados pela internet, e quais são os comportamentos seguros a fim de se proteger, diferentes situações podem acabar culminando em que caia vítima por falta de dar a devida importância ao assunto.

A rotina do dia a dia, esforço envolvido, e outros fatores, podem acabar trabalhando contra a intenção das pessoas de terem comportamentos mais seguros. Alguns hábitos como por exemplo a configuração segura de dispositivos, a avaliação de exposição nas redes sociais e aquisição de soluções de segurança digital envolvem tanto tempo quanto recursos financeiros. Por conseguinte, uma grande parcela da população acaba decidindo não se dar a este trabalho e esperar pelo melhor, porém com isso acabam sendo surpreendidas posteriormente ao ter suas redes sociais invadidas, ou perdendo consideráveis quantias monetárias em suas contas bancárias, em grande

[11] Apenas porque as pessoas estão cientes de algo não significa que elas se importarão. Mesmo que se importem e tenham a intenção de fazer a coisa certa, os contextos podem interferir no comportamento. (Tradução nossa).

Submissão #1843
Submetido em: 22/10/2025
Aprovado em: 31/03/2026

parte devido ao fato de que como expõe Kahneman (2013, p. 35) “Laziness is built deep inside our nature”[12].

Façamos por um momento o exercício mental de imaginar as possibilidades de um ataque cibernético direcionado a empresas de infraestruturas críticas, tomando por premissa que os trabalhadores que fazem parte da força de trabalho destes setores adotem comportamentos inseguros que permitam que este ataque seja bem-sucedido. Um clique em uma URL maliciosa e temos o cenário perfeito para um desastre de grandes proporções, afetando a vida de diversos cidadãos.

Em virtude disso, algumas ações podem ser tomadas com a finalidade de que situações que ponham os indivíduos em situação de risco no meio digital sejam evitadas, e assim a partir de comportamentos particulares dos cidadãos, fortalecer a nação como um todo devido ao resultado de uma soma de vários hábitos individuais seguros.

4. O ser humano como última linha de defesa

“If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand technology”[13]. Nesta citação, Scheneir (2015) resume bem um dos maiores problemas atuais no que tange a árdua tarefa de proteger os sistemas informáticos. Com o passar dos anos e a evolução das ferramentas de defesa, como por exemplo antivírus de nova geração, sistemas de detecção de intrusão, entre outros, a tendência puxada principalmente pelas indústrias é de dispender consideráveis quantias monetárias para ter o máximo de soluções de segurança possíveis. Entretanto, continua Schneier, “Security is a chain; the weakest link breaks it [...]”[14]. Não basta apenas estar na vanguarda com soluções de ponta. Se o operador dos sistemas informáticos – seja ele enquanto trabalhador ou como cidadão em sua vida particular - não tiver conhecimentos suficientes acerca das ameaças que exploram a parte humana da segurança digital, será na maioria das vezes o primeiro alvo a ser explorado, pois conforme Mitnick mencionado anteriormente, o investimento do criminoso é baixo e o risco quase nulo.

A segurança cibernética não é um produto, outrossim um processo, o qual envolve várias etapas e que começa com a hardenização dos humanos utilizadores dos sistemas digitais. Como ainda é impossível termos uma ferramenta que seja capaz de mitigar todo e qualquer tipo de ataque, torna-se mister ser ciber resiliente. Rothrock

[12] A preguiça está enraizada profundamente em nossa natureza. (Tradução nossa).
[13] Se você acha que a tecnologia pode resolver seus problemas de segurança, então você não entende os problemas e não entende a tecnologia. (Tradução nossa).
[14] A segurança é uma corrente; o elo mais fraco a quebra [...] (tradução nossa).

Submissão #1843
Submetido em: 22/10/2025
Aprovado em: 31/03/2026

(2018) expõe que "Security is about locking up and hunkering down. Resilience is about standing up to do business while fighting back"[15]. Similar a segurança digital, a resiliência digital não é uma solução de segurança que pode ser comprada e instalada. Como continua Rothrock (2018), "It's a state of mind and operational philosophy that, in due course, is destined to be embedded in all future management training, schooling, and corporations"[16]. Caso essa mentalidade não seja adotada, organizações e indivíduos estarão fadados ao fracasso.

Com isto, algumas oportunidades para apoiar neste processo de aumento da resiliência digital a nível nacional podem ser observadas.

4.1. Parcerias público x privadas

O governo federal enquanto promotor da PNED, por si só não tem ganho de alcance suficiente para promover mudanças num nível significativo para toda população. Com a maior parte da informação atual sendo consumida pela internet através de redes sociais na maioria dos casos, as pessoas tendem a levar em consideração o que o seu influencer ou youtuber favorito fala sobre determinado tema do que darem atenção a campanhas publicitárias de cunho educativo feitas pelo próprio governo. Por mais bem preparado e fácil de digerir que o conteúdo esteja, o lado afetivo tem grande relevância para que o comportamento seja aplicado de fato.

Perry (2018, p.75) comenta que campanhas de educação em segurança digital que surtem efeito são aquelas que fazem a conexão do intelectual com o emocional de uma pessoa. "[...] Once someone can intellectually and emotionally place themselves within the context of a situation, they are more likely to appreciate the meaning. And emotion allows the meaning to become rooted within the person's memory"[17]. Logo, podemos inferior que as personalidades mais estimadas por certo indivíduo podem ter papel relevante ao utilizar de seu carisma para transmitir este importante tópico.

Mesmo em um mundo mais adepto da internet como meio de comunicação, ainda há um público mais sênior que apesar de utilizá-la em seu dia a dia, ainda prefere a mídia televisiva tradicional para se informar. Para estes, podem ser utilizados os

[15] A segurança consiste em se trancar e se abrigar. A resiliência consiste em ficar de pé e operante enquanto revida. (Tradução nossa).
[16] É um estado de espírito e uma filosofia operacional que, no devido tempo, está destinada a ser incorporada em todos os futuros treinamentos de administração, escolas e empresas. (Tradução nossa).
[17] Quando uma pessoa consegue se situar intelectual e emocionalmente no contexto de uma situação, é mais provável que ela aprecie o significado. E a emoção permite que o significado se enraíze na memória da pessoa. (Tradução nossa).

Submissão #1843
Submetido em: 22/10/2025
Aprovado em: 31/03/2026

intervalos dos programas que possuem horário com maior audiência para inserir anúncios de curta duração, mas que criem esta conexão afetiva mencionada, posteriormente se enraizando no consciente e movendo a ação do espectador.

4.2. Empresas privadas

As empresas privadas têm papel importante na promoção de ações de educação cibernética. Seja por um interesse genuíno em fortalecer suas próprias defesas contra os ataques de criminosos, quanto para preencher requisitos regulatórios que as obriguem a isto, treinamentos sobre cibersegurança devem ser providos numa base regular a todos os funcionários para que assim possam ser peça fundamental da linha de defesa destas companhias.

Para que estas atividades de conscientização tenham sucesso em seu objetivo, que é causar uma mudança cultural auxiliando a que todos desenvolvam hábitos mais seguros, é necessário que as pessoas não apenas saibam o que fazer, mas que de fato apliquem no seu dia a dia. Muitas empresas tiveram sucesso utilizando programas de embaixadores, no qual funcionários dentro da organização se voluntariam para transmitir informações sobre segurança a outras equipes dentro da empresa. Os custos para desenvolverem programas como estes são baixos, o engajamento é alto devido ao senso de responsabilidade destes embaixadores, aumentam a escala pois a empresa terá mais pessoas transmitindo estas mensagens e com o aumento da maturidade em segurança, as pessoas começarão a ter mais senso de dever ao perceber comportamentos inseguros e reportá-los para que providências sejam tomadas.

Estes programas não apenas causam impacto na cultura local da empresa, mas como os funcionários têm participação ativa acabam por absorver vários conteúdos relevantes acerca do tema, e posteriormente acabam replicando estes comportamentos seguros e transmitindo a importância de dar atenção para o tema a pessoas que fazem parte do seu círculo de amigos e familiares, desta forma contribuindo indiretamente para o aumento da resiliência cibernética nacional.

4.3. Fundações sem fins lucrativos

Apesar de ter políticas voltadas para a educação digital, o poder público não tem recursos suficientes para poder causar o impacto necessário na vida dos cidadãos em tempo de acompanhar o passo da evolução das tecnologias. Como argumenta Duarte (2024, p.98) “Não há condições de se comparar uma escola [...] privada [...] com uma escola periférica em que as vezes não há nem giz para escrever no quadro”. Este cenário fomenta a desigualdade digital entre a parcela da sociedade que possui mais recursos

Submissão #1843
Submetido em: 22/10/2025
Aprovado em: 31/03/2026

em relação a aquela que muito pouco ou nada tem. Isto se refletirá cedo ou tarde, pois a falta da preparação necessária em segurança digital será demonstrada quando estes cidadãos forem utilizar novas tecnologias, seja para seu trabalho ou lazer.

Fundações sem fins lucrativos como por exemplo a iniciativa WOMCY (Latam Women in Cybersecurity)[18] voltada não somente para mulheres como o nome indica, mas também para crianças em idade escolar e estudantes universitários, tem levado informação sobre ameaças a segurança cibernética e introduzido o público no ecossistema digital. Conforme a missão da entidade em seu próprio website, a intenção com esta iniciativa é minimizar a brecha de conhecimento.

Iniciativas menores a nível municipal e que contam com voluntários do setor de tecnologia também tem levado conhecimento sobre segurança digital a estudantes da rede pública de ensino, a fim de reduzir a lacuna de conhecimento entre instituições públicas e privadas e aumentando por fim a maturidade de segurança cibernética desde a infância. Estas atividades se refletirão futuramente em uma sociedade mais ciber resiliente, à medida que estas crianças forem crescendo e desempenhando atividades como futuros cidadãos e trabalhadores.

4.4. Legislação

Wendt (2023, p. 132) observa que mesmo desconhecendo as normativas já existentes acerca da internet no Brasil, a cultura brasileira é a da regulamentação, na qual o Direito tem papel relevante na resolução de conflitos, incluindo aqui aqueles advindos do ambiente digital, em resumo, crimes praticados no ambiente cibernético.

Ainda que legislações acerca do ambiente cibernético não sejam relativamente tão novas no Brasil, começando inicialmente em 1987 com a Lei nº 7.646 (Lei de Software, revogada) que abordava condutas de violação de programas de computador em seus artigos 35 e 37, e tendo notoriedade pública mais recentemente com a sanção da Lei nº 12.737 de 2012, conhecida também como ‘Lei Carolina Dieckmann’, ainda há questões conceituais e redacionais das leis que tangem a tipificação de crimes cibernéticos que podem gerar margem a diferentes interpretações, resultando em frustração para o policial enquanto investigador cibernético e em um sentimento de falta de efetividade devido a tipificação penal, conforme observa Wendt (2023, p.149 – 153).

Somado a estes fatores, Wendt (2023, p.191) observa que:

[18] Vide https://womcy.org/pt/

Submissão #1843
Submetido em: 22/10/2025
Aprovado em: 31/03/2026

> *[...] não há protocolo básico do atendimento de ocorrências em que os atos criminosos são cometidos com o uso da Internet, nem de como preservar essas evidências, carecendo a estrutura administrativa de uma padronização e uniformidade.*

A criação do Plano Tático de Combate a Crimes Cibernéticos do MJSP em 2022, teve como intento resolver entre outros, a esta lacuna mencionada, porém até o final deste mesmo ano, ainda não havia sido consolidado um modelo padrão para atendimento de ocorrências e preservação de provas digitais conforme Wendt destaca (2023, p.192). Nesta falta de padronização processual, o agente da lei não consegue desempenhar suas atividades eficazmente, tornando o apoio ao cidadão moroso e nem sempre satisfatório ao ponto de vista do requerente. Em vista disso, se vê a necessidade da continuidade de ações técnicas neste âmbito para que as expectativas da sociedade estejam alinhadas com as capacidades de resposta dos investigadores.

Se fato é que a sociedade espera das forças da lei efetividade na investigação, quanto espera do Legislativo penas mais severas para criminosos que agem no ambiente digital, faz-se mandatório que haja mais interlocução entre estas duas partes. Os agentes da lei devem inteirar-se acerca dos projetos que visem melhorar sua realidade investigativa (Wendt, 2023, p. 231) e comunicar quaisquer preocupações ao Legislativo e Judiciário, que por sua vez deve avaliar as proposições nos melhores interesses dos cidadãos como requerentes, - uma vez que são representantes por estes eleitos –assim revisando as normativas e leis que englobam este processo com intuito de torná-lo cada vez mais eficiente e eficaz.

Com a implementação de novas tecnologias virão outros tipos de situações não previstas nas leis já existentes, sendo necessário atualizá-las com estes novos mecanismos, e uma cada vez mais forte coesão entre todas as entidades (políticas, judiciárias) que devem zelar pela segurança e bem-estar dos cidadãos brasileiros será necessária. Só assim será possível enfrentar o crime informático, que já está muito bem-organizado.

5. Considerações finais

A cada ano que passa, as ameaças ao mundo digital têm ficado cada vez mais em evidência devido aos impactos sociais e econômicos causados por ataques criminosos. O Fórum Econômico Mundial em sua 19ª Edição do Relatório Global de Riscos (2024, p. 13), reporta que em 2024 os ataques cibernéticos ocupam a 5ª posição no panorama de riscos, com uma previsão de subida para 4º lugar até 2026, mostrando assim a relevância do tema a nível mundial.

Submissão #1843
Submetido em: 22/10/2025
Aprovado em: 31/03/2026

A teoria do Caminho mais curto ou da Oportunidade, conforme Felson (1994), expõe que os crimes ocorrem quando três elementos se encontram: um indivíduo propenso a cometer o crime, um alvo vulnerável e a ausência de um guardião capaz de proteger o alvo. Esta aplica-se também ao ecossistema digital e as estatísticas de crimes eletrônicos são prova disso. Poucos são os guardiões capacitados, muitos são os alvos incautos. E a falta de percepção da punibilidade contra crimes digitais, bem como o relativo afastamento moral em vista do meio que o crime é praticado, faz com que indivíduos mal-intencionados tenham o cenário ideal para que possam consumar o ato.

Apesar do aumento em investimentos em novas tecnologias cada vez mais avançadas para proteger este intrincado ecossistema, ainda se veem ataques bem-sucedidos. Estes têm se aproveitado na maioria dos casos de fragilidades no comportamento humano, seja pela curiosidade, ingenuidade ou falta de senso de dever em proteger as organizações que estão inseridos e até mesmo em sua vida familiar. O custo de planejamento de um ataque de engenharia social é extremamente menor para um criminoso se comparado ao esforço de pesquisa de vulnerabilidades em equipamentos tecnológicos, e as chances de sucesso explorando psicologicamente as pessoas são muito maiores.

Desde os tempos mais primórdios o ser humano tem se aproveitado de técnicas de persuasão para alcançar seus objetivos, sejam estes éticos e para o bem-estar de seu próprio semelhante, quer sejam com propósitos escusos, visando obter vantagens indevidas. Hábitos humanos, portanto, tem o poder de aumentar as defesas contra a utilização de ataques que se valem destes mecanismos, caso sejam devidamente trabalhados e com apoio de diversos mecanismos sociais. Desta forma, o que antes era o alvo em ataques, passa a se tornar a melhor defesa contra estes.

Atingir a resiliência cibernética é um desafio complexo tanto para organizações privadas quanto para Estados, desafio este que requer uma abordagem multidisciplinar. Antes de investimentos em tecnologia, deve-se sobretudo educar os operadores de sistemas, para que na eventual falha de algum mecanismo tecnológico de proteção, o ser humano ainda assim consiga perceber as nuances que possam indicar uma possível tentativa de exploração ao ambiente digital no qual ele está alocado.

Uma nação que é ciber resiliente começa com cidadãos ciber instruídos. Tratando-se de um grande país em extensão territorial, o Brasil através de seu governo federal ainda tem uma grande maratona a percorrer para que a maioria da sua população tenha condições mínimas de utilizar sistemas informáticos com segurança. Se as ações

Submissão #1843
Submetido em: 22/10/2025
Aprovado em: 31/03/2026

de educação não ficarem somente a cargo do governo, e continuarem contando com apoio de outras organizações civis que já estão fazendo sua parte, certamente avanços rumo a um país mais seguro digitalmente serão sentidos a médio e longo prazo.

Esta resiliência cibernética inclui também a capacidade de resposta à eminência e materialização de ataques no meio digital, sejam eles direcionados a organizações e infraestruturas críticas afetando assim uma ampla gama de pessoas, sejam de âmbito particular como por exemplo nas fraudes 'cotidianas'. Esta resposta envolve as forças de criação e aplicação das leis. Somente com o mecanismo Legislativo, Judicial e investigativo – aqui representantes deste mecanismo de resposta - trabalhando em conjunto para os melhores interesses da sociedade, ter-se-á formas de impedir o avanço desenfreado da criminalidade digital.

Quando a educação digital – prevenção – for suficientemente impactante para que os cidadãos nativamente saibam 'o quê' fazer para estarem seguros no mundo digital, e as forças de lei – resposta - tiverem a seu dispor todos os mecanismos necessários para aplicabilidade de punições que desmotivem o comportamento criminoso, o Brasil começará a ter menores índices de crimes praticados digitalmente e passará a ser mais resiliente ciberneticamente.

Referências

AIKEN, Mary. The Cyber Effect: A Pioneering Cyberpsychologist Explains How Human Behavior Changes Online. Random House, 2018.

BRASIL. Decreto Nº 9.573, de 22 de Novembro de 2018. Aprova a Política Nacional de Segurança de Infraestruturas Críticas. In: Diário Oficial da República Federativa do Brasil, Brasília, DF, 23 nov. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9573.htm. Acesso em: 29 abr. 2024.

BRASIL. Governo Federal lança Plano Tático de Combate a Crimes Cibernéticos. Ministério da Justiça e Segurança Pública, 23/03/2022a. Disponível em: https://www.gov.br/pt-br/noticias/justica-e-seguranca/2022/03/governo-federal-lanca-plano-tatico-de-combate-a-crimes-ciberneticos. Acesso em: 26 maio 2024.

BRASIL. Lei Nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. In: Diário Oficial da República Federativa do Brasil, Brasília, DF, 30 nov. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 26 maio 2024.

BRASIL. Lei Nº 14.155, de 27 de maio de 2021b. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei

Submissão #1843
Submetido em: 22/10/2025
Aprovado em: 31/03/2026

nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. In: Diário Oficial da República Federativa do Brasil, Brasília, DF, 27 maio 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14155.htm. Acesso em: 26 maio 2024.

BRASIL. Lei Nº 15.533, de 11 de Janeiro de 2023. Institui a Política Nacional de Educação Digital. In: Diário Oficial da República Federativa do Brasil, Brasília, DF, 11 jan. 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Lei/L14533.htm. Acesso em: 29 abr. 2024.

CARPENTER, Perry. Transformational Security Awareness: What Neuroscientists, Storytellers, and Marketers Can Teach Us About Driving Secure Behaviors. Wiley, 2018.

CNN. Golpistas usam deepfake de diretor financeiro e roubam US$ 25 milhões. Disponível em: https://www.cnnbrasil.com.br/economia/negocios/golpistas-usam-deepfake-de-diretor-financeiro-e-roubam-us-25-milhoes/. Acesso em: 04 maio 2024.

DIMAGGIO, John. The Art of Cyberwarfare. No Starch Press, 2022.

DRAGOS. OT Cybersecurity: The 2023 Year In Review. 2024. Disponível em: https://hub.dragos.com/hubfs/312-Year-in-Review/2023/Dragos-2023-Year-in-Review-Full-Report.pdf?hsLang=en. Acesso em: 30 abr. 2024.

DUARTE, Marcela. Política Nacional de Educação Digital: Propostas, Desafios e Estratégias para a Promoção da Inclusão Digital e do Uso da Tecnologia na Educação. Direito e TI, Porto Alegre, v2, nº 18, abr. 2024.

FELSON, Marcus. Crime and Everyday Life: Insights and Implications for Society. Pine Forge Press, 1994.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. 17º Anuário Brasileiro de Segurança Pública. São Paulo: Fórum Brasileiro de Segurança Pública, 2023. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2023/07/anuario-2023.pdf. Acesso em: 30 abr. 2024.

GREENBERG, Andy. Sandworm Hackers Caused Another Blackout in Ukraine—During a Missile Strike. WIRED, 2023. Disponível em: https://www.wired.com/story/sandworm-ukraine-third-blackout-cyberattack/. Acesso em: 30 abr. 2024.

HADNAGY, Christopher. Social Engineering: The Science of Human Hacking. 2. ed. Wiley, 2018.

KAHNEMAN, Daniel. Thinking, Fast and Slow. Farrar Straus Giroux, 2013.

KOSFELD, Michael, HEINRICHS, Markus, ZAK, Paul. et al. Oxytocin increases trust in humans. Nature, nº 435, abr./maio 2005. Disponível em: https://doi.org/10.1038/nature03701. Acesso em: 30 abr. 2024.

Submissão #1843
Submetido em: 22/10/2025
Aprovado em: 31/03/2026

MITNICK, Kevin. The Art of Deception: Controlling the Human Element of Security. Wiley, 2002.

ROTHROCK, Ray. Digital Resilience: Is your company ready for the next cyber threat? Amacom, 2018.

SCHNEIER, Bruce. Liars and Outliers: Enabling the Trust that Society Needs to Thrive. Wiley, 2012.

SCHNEIER, Bruce. Secrets and Lies: Digital Security in a Networked World. 15. Ed. Wiley, 2015.

WEF, World Economic Forum. Global Risks Report 2024. Disponível em: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf. Acesso em: 11 maio 2024.

WENDT, Emerson. As expectativas cognitivas e normativas dos atores de investigação policial em face dos crimes cibernéticos. 2023. Tese (Doutorado em Direito) – Universidade LaSalle, Canoas, 2023.

WOMCY, Latam Women in Cybersecurity. Início. Disponível em: https://womcy.org/pt/. Acesso em: 11 maio 2024.

Digital security and national cyber resilience

Abstract

Cyber resilience is crucial for national security, as a country vulnerable to cyber attacks can suffer serious economic, political, and social consequences. In this context, this research investigates how the digital security perception of Brazilians affects national cyber resilience. The study focuses on understanding how behavioral, social, and psychological aspects influence this perception and how cyber security awareness and education practices can be improved. The central hypothesis is that the digital security perception is directly linked to these aspects, which is reflected in safe or unsafe online habits and, consequently, affects the country's cyber resilience. The objective is to identify the factors that influence the digital security perception and propose strategies to elevate national cyber security maturity. Additionally, the research contributes to understanding the role of individual perceptions in a country's cyber security, highlighting the importance of specific educational and awareness approaches. The adopted methodology is bibliographic research, which allows the analysis and synthesis of existing knowledge on the subject.

Keywords

Digital. Infrastructure. Resilience. Security. Society.

Seguridad digital y la resiliencia cibernética nacional

Resumen

La resiliencia cibernética es vital para la seguridad nacional, y esta investigación explora cómo la percepción de seguridad digital de los brasileños la afecta. El estudio se centra en aspectos

Submissão #1843
Submetido em: 22/10/2025
Aprovado em: 31/03/2026

conductuales, sociales y psicológicos que moldean esta percepción, influyendo en hábitos en línea seguros o inseguros. La hipótesis central es que esta percepción está directamente ligada a estos factores, impactando la resiliencia cibernética del país. El objetivo es identificar los elementos que influyen en la percepción de seguridad digital y proponer estrategias para mejorar la madurez de la seguridad cibernética nacional. La investigación, basada en una revisión bibliográfica, destaca la importancia de enfoques educativos y de concienciación para fortalecer la seguridad cibernética individual y colectiva.

Palabras clave

Digital. Infraestructura. Resiliencia. Seguridad. Sociedad.

Como citar

WENDT, E.; GRASEL, C. H. Segurança digital e a resiliência cibernética nacional. **Revista Jurídica da FA7**, Fortaleza, v. 22, n. 1, p. 148-168, jan./abr. 2025.