



**UNIVERSIDADE
KIMPA VITA**

15 - 10 | 2026

Os utilizadores finais e a segurança da informação: comportamentos, conformidade e contexto organizacional

*End Users and Information Security: Behaviour, Compliance, and
Organisational Context*

Nsitukemba Vieira Viegas

Versão electrónica

URL: <https://ciencia.unikivi.ao/>

Data de publicação: 15-10-2026. Páginas: 13

Editor

Revista Científica Interdisciplinar da UNIKIVI

Referência eletrónica

Viegas, N. V. (2026). Os utilizadores finais e a segurança da informação: comportamentos, conformidade e contexto organizacional. Revista da UNIKIVI. 2024. 01(01), 01-13.



OS UTILIZADORES FINAIS E A SEGURANÇA DA INFORMAÇÃO: COMPORTAMENTOS, CONFORMIDADE E CONTEXTO ORGANIZACIONAL

End Users and Information Security: Behaviour, Compliance, and Organisational Context

Nsitukemba Vieira Viegas

Access Holdings Plc, Nigéria

situkemba@gmail.com | <https://orcid.org/0000-0003-1891-9093>

RESUMO

Os impactos associados a práticas inadequadas de segurança da informação continuam a constituir, um desafio relevante para as organizações e para a sociedade, tornando necessário compreender os factores humanos envolvidos na protecção dos activos de informação. Apesar da evolução dos mecanismos técnicos de protecção, os comportamentos dos utilizadores continuam a assumir particular importância na exposição das organizações a incidentes de segurança. Neste contexto, o presente trabalho tem como objectivo analisar o papel dos factores humanos na segurança da informação, considerando as dimensões individual, organizacional e social. Adoptou-se uma abordagem qualitativa, de natureza exploratória e conceptual, baseada numa revisão e síntese crítica da literatura científica relevante, complementada pela experiência profissional do autor no domínio da auditoria de sistemas de informação. A análise da literatura permitiu identificar diferentes formas de conformidade e não conformidade relativamente às práticas de segurança, bem como factores individuais e organizacionais associados aos comportamentos dos utilizadores. Os contributos analisados sugerem que a segurança da informação não depende exclusivamente da implementação de controlos tecnológicos, mas também da articulação entre políticas de segurança, cultura organizacional, formação, percepção do risco e práticas quotidianas dos utilizadores. Neste sentido, a segurança da informação pode ser compreendida como um fenómeno sócio-técnico, no qual factores tecnológicos e humanos se encontram estreitamente relacionados. Conclui-se que o reforço da cultura de segurança, a sensibilização e capacitação dos utilizadores e a integração entre medidas técnicas e organizacionais constituem elementos importantes para promover comportamentos mais seguros e fortalecer a resiliência das organizações perante as ameaças digitais contemporâneas.

Palavras-chave: Segurança da Informação; Factores Humanos; Comportamento dos Utilizadores; Conformidade; Auditoria de Sistemas; Abordagem Sócio-Técnica.

ABSTRACT

The impacts associated with inadequate information security practices continue to be a significant challenge for organizations and society, making it necessary to understand the human factors involved in protecting information assets. Despite the evolution of technical protection mechanisms, user behaviors still play a particularly important role in exposing organizations to security incidents. In this context, this work aims to analyze the role of human factors in information security, considering the individual, organizational, and social dimensions. A qualitative approach was adopted, exploratory and conceptual in nature, based on a review and critical synthesis of the

relevant scientific literature, complemented by the author's professional experience in the field of information systems auditing. The literature review made it possible to identify different forms of compliance and non-compliance regarding security practices, as well as individual and organizational factors associated with user behaviors. The analyzed contributions suggest that information security does not rely solely on the implementation of technological controls, but also on the coordination between security policies, organizational culture, training, risk perception, and users' everyday practices. In this sense, information security can be understood as a socio-technical phenomenon, where technological and human factors are closely interconnected. It is concluded that strengthening a security culture, raising awareness and training users, and integrating technical and organizational measures are important elements for promoting safer behaviors and enhancing the resilience of organizations against contemporary digital threats.

Keywords: Information Security; Human Factors; User Behavior; Compliance, Systems Auditing; Sócio-Technical Approach.

1 INTRODUÇÃO

A evolução das tecnologias da informação e comunicação tem transformado profundamente a forma como as organizações desenvolvem as suas actividades, armazenam informação e prestam serviços. A crescente interligação entre sistemas, dispositivos e plataformas digitais tornou os ambientes tecnológicos mais complexos e, simultaneamente, mais expostos a diferentes formas de ameaça. Tecnologias emergentes, como a Internet das Coisas (*Internet of Things* – IoT), ilustram esta realidade ao ampliar o número e a diversidade de dispositivos conectados. Como consequência, aumenta também a superfície de ataque e torna-se mais exigente a identificação, avaliação e gestão dos riscos associados à segurança da informação.

Esta transformação tecnológica, contudo, não tem sido acompanhada por uma evolução equivalente dos comportamentos relacionados com a protecção da informação. No quotidiano das organizações, situações como *phishing*, engenharia social, utilização inadequada de credenciais, erros operacionais e incumprimento de políticas internas continuam a constituir importantes fontes de exposição. O *Data Breach Investigations Report* da Verizon tem evidenciado a presença recorrente de factores humanos nos incidentes de segurança analisados, reforçando a necessidade de compreender o comportamento dos utilizadores como parte integrante da segurança da informação (Verizon, 2024).

Esta perspectiva implica ultrapassar a ideia de que o utilizador constitui apenas uma vulnerabilidade do sistema. Embora determinadas acções humanas possam aumentar a exposição ao risco, os utilizadores também podem contribuir para a prevenção, detecção e resposta a incidentes. A segurança depende, em grande medida, da forma como as pessoas compreendem os riscos, interpretam as políticas e incorporam as práticas de segurança nas suas actividades quotidianas (Furnell & Rajendran, 2012; Guo, 2013).

Os mecanismos tecnológicos, como *firewalls*, sistemas de detecção e controlos de acesso, permanecem indispensáveis. Todavia, a sua eficácia encontra-se relacionada com a forma como são concebidos, implementados e utilizados. Factores como conhecimento, percepção do risco, atitudes, consciência de segurança, formação, cultura, organizacional e conformidade podem condicionar a relação dos indivíduos com os sistemas de informação (Guo, 2013; Safa et al., 2015).

É neste ponto que se situa o contributo do presente estudo. Em vez de analisar isoladamente a tecnologia ou o comportamento individual, propõe-se uma leitura multinível, articulando factores individuais, organizacionais e sociais. Esta perspectiva permite compreender que os comportamentos de segurança não surgem no vazio: são desenvolvidos num determinado contexto, influenciados pelas características dos indivíduos, pelas práticas de gestão, pelas políticas institucionais e pelas condições em que o trabalho é realizado.

Assim, o presente trabalho tem como objectivo analisar o papel dos factores humanos na segurança da informação, numa perspectiva multinível que contempla as dimensões individual, organizacional e social. Para esse efeito, procede-se a uma revisão e síntese crítica da literatura científica, procurando identificar os principais factores associados aos comportamentos de

segurança, os modelos conceptuais utilizados para os explicar e as implicações desses contributos para a gestão organizacional da segurança da informação.

O artigo encontra-se organizado em cinco secções principais. Após a introdução, apresenta-se a metodologia utilizada na revisão da literatura. Seguidamente, são expostos os principais resultados da análise, organizados em função das dimensões individual e organizacional. A discussão confronta esses contributos e procura retirar as principais implicações teóricas e práticas. Por fim, apresentam-se as conclusões e algumas propostas para futuras investigações.

2 MÉTODOS

2.1 Abordagem e desenho da investigação

O presente estudo adopta uma abordagem qualitativa, de natureza exploratória e conceptual, desenvolvida através de uma revisão narrativa e crítica da literatura científica sobre segurança da informação, com particular atenção aos factores humanos, comportamentais e organizacionais associados à utilização dos sistemas de informação em contexto institucional. Esta opção metodológica permite reunir, interpretar e relacionar diferentes contributos teóricos, identificando convergências, divergências e lacunas na investigação existente. Ao contrário de uma revisão meramente descritiva, a revisão crítica procura interpretar os conhecimentos disponíveis e construir uma síntese conceptual coerente (Grant & Booth, 2009; Snyder, 2019).

A abordagem qualitativa justifica-se pelo facto de o estudo não pretender quantificar comportamentos nem testar relações causais entre variáveis. O objectivo consiste em compreender de que modo factores como conhecimento, percepção do risco, atitudes, consciência de segurança, cultura organizacional, liderança, políticas institucionais e formação são abordados e relacionados na literatura especializada. Esta perspectiva é compatível com a compreensão da segurança da informação como um fenómeno sociotécnico, no qual os mecanismos tecnológicos interagem com factores individuais e organizacionais (Guo, 2013; Safa et al., 2015; Khadka & Ullah, 2025).

2.2 Pesquisa e identificação da literatura

A pesquisa bibliográfica foi realizada nas bases de dados académicas Scopus, Web of Science e IEEE Xplore, consideradas relevantes para as áreas dos sistemas de informação, segurança da informação e ciber-segurança. Foram privilegiadas publicações produzidas entre 2015 e 2025, sem excluir estudos anteriores considerados fundamentais para a construção do enquadramento conceptual. Entre estes, destacam-se Guo (2013), pelo contributo para a compreensão do comportamento relacionado com a segurança dos sistemas de informação no local de trabalho, e Safa et al. (2015), pelo estudo da formação de comportamentos conscientes de segurança nas organizações.

A estratégia de pesquisa utilizou descritores em Língua Inglesa, considerando a predominância da produção científica internacional neste domínio. Foram utilizados termos como *information security*, *cybersecurity*, *human factors*, *user behaviour*, *security awareness*, *security compliance*, *organizational culture*, *information security management* e *cybersecurity behaviour*, combinados através dos operadores booleanos AND e OR. A escolha destes descritores procurou abranger as dimensões individual, comportamental, tecnológica e organizacional da segurança da informação (Alshaikh, 2021; Renaud et al., 2022; Sutton & Tompson, 2025).

2.3 Critérios de inclusão e exclusão

Foram incluídos artigos científicos revistos por pares, trabalhos publicados em revistas especializadas, actas de conferências e estudos académicos que apresentassem contributos relevantes para a compreensão dos factores humanos, comportamentais ou organizacionais relacionados com a segurança da informação e a ciber-segurança.

A selecção incidiu particularmente sobre estudos relacionados com consciência de segurança, comportamento dos utilizadores, conformidade com políticas, percepção do risco, atitudes, cultura organizacional, liderança, formação e gestão da segurança da informação. Esta delimitação encontra suporte em estudos que apontam a consciência, a cultura organizacional, o

apoio da gestão e as atitudes dos trabalhadores como factores relevantes para a formação de comportamentos de segurança (Safa et al., 2015; Alshaikh, 2021; Sutton & Tompson, 2025).

Foram excluídos textos de opinião sem fundamentação científica, documentos sem relação directa com o objecto da investigação e estudos exclusivamente técnicos que não apresentassem qualquer dimensão humana, comportamental ou organizacional. Estes critérios permitiram preservar a coerência temática e manter o foco na relação entre utilizadores, organizações e práticas de segurança.

2.4 Selecção e análise da literatura

O processo de selecção iniciou-se com a análise dos títulos, resumos e palavras-chave, seguindo-se a leitura integral dos trabalhos considerados pertinentes. Os estudos seleccionados foram posteriormente organizados segundo três níveis de análise: individual, organizacional e social.

No nível individual, foram considerados factores como conhecimento, atitudes, percepção do risco, consciência de segurança, experiência e tomada de decisão. No nível organizacional, analisaram-se a cultura de segurança, liderança, políticas institucionais, formação, supervisão e mecanismos de controlo. O nível social contemplou a influência do contexto mais amplo, das experiências sociais e das transformações do ambiente digital sobre a percepção e resposta dos indivíduos às ameaças de segurança.

A análise assumiu uma natureza temática, comparativa e interpretativa, procurando identificar padrões, convergências e divergências entre os estudos. Mais do que apresentar os trabalhos isoladamente, procurou-se relacionar os conceitos e factores identificados para construir uma interpretação integrada do comportamento de segurança (Grant & Booth, 2009; Snyder, 2019). Particular atenção foi dada à relação entre factores individuais e organizacionais, considerando que a conformidade com as políticas de segurança não depende exclusivamente das características dos utilizadores, mas também do apoio da gestão, da cultura institucional e da forma como as medidas de segurança são percebidas pelos trabalhadores (Delso-Vicente et al., 2025).

2.5 Natureza dos dados e delimitação metodológica

Não foram recolhidos dados empíricos primários. Consequentemente, os resultados apresentados correspondem a uma síntese conceptual e crítica da literatura seleccionada, não constituindo evidência empírica produzida directamente pelo estudo. A experiência profissional do autor em auditoria de sistemas de informação foi utilizada apenas como elemento complementar de reflexão e contextualização, não sendo considerada uma fonte autónoma de evidência científica.

Por fim, não se pretendeu realizar uma revisão sistemática nem uma análise bibliométrica, uma vez que não foi adoptado um protocolo de pesquisa exaustiva, avaliação formal da qualidade metodológica dos estudos ou quantificação da produção científica. O propósito consistiu em integrar criticamente contributos relevantes, identificar convergências e divergências e construir uma interpretação coerente sobre a relação entre factores humanos, comportamento dos utilizadores, contexto organizacional e segurança da informação (Grant & Booth, 2009; Khadka & Ullah, 2025; Snyder, 2019).

3 RESULTADOS

3.1 Segurança da informação e utilizadores finais

A informação constitui um dos activos mais importantes das organizações, pelo que a sua protecção representa um dos principais desafios da gestão contemporânea dos sistemas de informação. Embora as organizações invistam em mecanismos tecnológicos, como sistemas de controlo de acesso, software especializado e soluções de protecção de redes e dados, a segurança não depende exclusivamente da tecnologia. O comportamento dos utilizadores pode influenciar significativamente a protecção dos activos informacionais (Guo, 2013; Ögütçü et al., 2016).

Os utilizadores finais assumem particular relevância por interagirem directamente com sistemas, aplicações, redes e dados organizacionais. Comportamentos inadequados, negligentes ou intencionalmente prejudiciais podem aumentar a exposição a riscos e incidentes de segurança. Guo (2013) identifica diferentes comportamentos relacionados com a segurança, incluindo práticas de protecção, conformidade, comportamentos de risco e comportamentos potencialmente danosos. Assim, o utilizador não deve ser considerado apenas uma fonte de vulnerabilidade, mas um elemento cujo comportamento pode contribuir tanto para a segurança como para a ocorrência de incidentes.

A consciência e o conhecimento dos utilizadores constituem igualmente factores determinantes. Segundo Ögütçü et al. (2016), os comportamentos de risco estão relacionados com o nível de consciência sobre a segurança da informação, sendo influenciados pelos hábitos de utilização da Internet e pela percepção dos riscos. Neste contexto, a formação e a sensibilização assumem um papel estratégico, pois a existência de políticas e mecanismos técnicos não garante, por si só, comportamentos seguros. Os utilizadores devem compreender os riscos, conhecer as políticas institucionais e desenvolver competências para reconhecer e responder adequadamente a ameaças, incluindo tentativas de engenharia social (Ghafir et al., 2018; Albladi & Weir, 2018).

A segurança da informação deve, portanto, ser entendida como um fenómeno **socio-técnico**, resultante da interacção entre tecnologia, pessoas e organização. A cultura de segurança influencia a forma como os indivíduos percebem os riscos e assumem responsabilidades na protecção da informação (Glaspie & Karwowski, 2018).

Nesta perspectiva, o utilizador final deve ser considerado também um agente activo de protecção, mediante o cumprimento das políticas de segurança, a utilização responsável dos sistemas e a comunicação de actividades suspeitas. Consequentemente, a gestão da segurança da informação exige uma abordagem integrada, que articule tecnologia, políticas institucionais, formação, sensibilização, cultura organizacional e responsabilização dos utilizadores.

3.2 Comportamento humano e Segurança da informação

Os estudos sobre o comportamento relacionado com a segurança da informação apresentam diferentes formas de classificação. Algumas abordagens distinguem comportamentos intencionais e não intencionais, enquanto outras consideram a origem da ameaça, a motivação, o nível de conhecimento exigido ou o grau de conformidade com as normas e políticas organizacionais (Furnell & Rajendran, 2012; Pimenta et al., 2016). Esta diversidade reflecte o carácter multifacetado do comportamento humano, influenciado por factores individuais, organizacionais e contextuais (Herath & Rao, 2009; Bulgurcu et al., 2010).

Consequentemente, não existe um único padrão de comportamento inseguro. Um erro involuntário, decorrente de desconhecimento, falta de atenção ou dificuldades na utilização de um sistema, apresenta natureza e implicações diferentes de uma violação deliberada de uma política de segurança. Do mesmo modo, o incumprimento de procedimentos pode resultar de insuficiente conhecimento, dificuldades práticas, hábitos inadequados ou de uma decisão consciente de contornar as regras (Vance et al., 2012). A conformidade depende, assim, de factores como a percepção dos riscos, as atitudes, a auto-eficácia, as normas sociais e a avaliação das consequências do cumprimento ou incumprimento (Bulgurcu et al., 2010; Herath & Rao, 2009).

Neste sentido, a conformidade não deve ser analisada apenas numa perspectiva binária de “cumpre” ou “não cumpre”. O comportamento pode ser compreendido como um **continuum**, que se estende desde a consciência e aceitação das normas até situações de negligência, resistência ou violação deliberada. Os hábitos e comportamentos anteriormente adquiridos podem igualmente influenciar a adopção ou rejeição das práticas de segurança (Vance et al., 2012).

Esta distinção possui implicações práticas para a gestão da segurança. Comportamentos associados ao desconhecimento ou erro devem ser enfrentados através de formação, sensibilização, comunicação e simplificação dos procedimentos. Comportamentos deliberadamente contrários às políticas exigem mecanismos adequados de controlo, monitorização e responsabilização. Assim, a classificação dos comportamentos deve orientar intervenções diferenciadas, proporcionais às suas causas, natureza e gravidade.

3.3 Contexto organizacional e cultura de segurança

Os estudos analisados evidenciam a importância do contexto organizacional na formação dos comportamentos relacionados com a segurança da informação. A conformidade dos utilizadores com as políticas de segurança não depende apenas de características individuais, sendo também influenciada pela cultura organizacional, liderança, normas sociais, comunicação, formação e percepção das consequências do cumprimento ou incumprimento das regras (Herath & Rao, 2009; Bulgurcu et al., 2010; Safa et al., 2015). Assim, os comportamentos podem variar entre a aceitação e interiorização das normas e situações de negligência, resistência ou incumprimento deliberado.

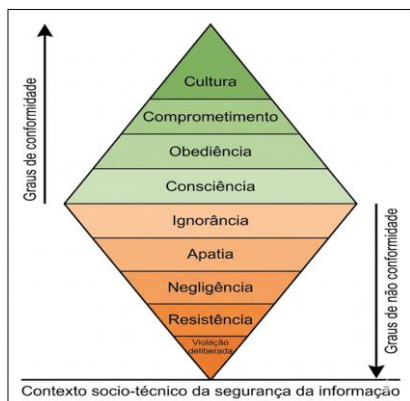
A conformidade resulta da interacção entre factores individuais e organizacionais, incluindo atitudes, consciência de segurança, auto-eficácia e percepção dos benefícios e custos associados ao cumprimento das políticas (Bulgurcu et al., 2010; Safa et al., 2015). Por conseguinte, a existência formal de políticas não garante a sua aplicação efectiva nas práticas quotidianas.

Entre os principais factores organizacionais destacam-se a cultura de segurança, a liderança, a clareza das políticas, a formação, a sensibilização, a comunicação e os mecanismos de supervisão. A cultura de segurança compreende valores, pressupostos e práticas partilhadas que orientam a percepção e a responsabilidade dos membros da organização relativamente à protecção da informação (Da Veiga & Eloff, 2010; Glaspie & Karwowski, 2018). Uma cultura sólida favorece comportamentos seguros, enquanto uma cultura frágil pode contribuir para práticas inadequadas.

Deste modo, a conformidade deve ser entendida como um processo organizacional contínuo. Uma cultura de segurança consolidada pode favorecer a interiorização das práticas de protecção da informação, transformando a segurança num valor partilhado e numa responsabilidade colectiva (AlHogail, 2015). O seu reforço exige a articulação entre liderança, políticas, formação, comunicação, supervisão e participação activa dos utilizadores.

Figura 1

Níveis de conformidade de segurança numa organização.



Fonte: Elaboração própria com base em Da Veiga e Eloff (2010), AlHogail (2015) e Glaspie e Karwowski (2018).

A Figura 1 apresenta uma representação conceptual dos diferentes níveis de conformidade e não conformidade relacionados com a segurança da informação em contexto organizacional. A representação é estruturada como um contínuo comportamental, permitindo compreender que os utilizadores não se posicionam necessariamente em categorias rígidas de “cumpridores” ou “incumpridores”. Os comportamentos podem variar em função do conhecimento, da consciência, da motivação, das atitudes, das condições organizacionais e da percepção dos riscos e das consequências associados às práticas de segurança (Guo, 2013; Bulgurcu et al., 2010; Safa et al., 2015).

Na dimensão da conformidade, são representados níveis progressivos que vão da consciência das regras à obediência, ao comprometimento e, num nível mais elevado, à interiorização da segurança como valor organizacional. Esta progressão conceptual traduz a passagem do conhecimento das políticas para a adopção efectiva e consistente de

comportamentos seguros. A literatura demonstra que a consciência e a percepção das políticas de segurança constituem factores importantes para a conformidade dos utilizadores, embora a existência de conhecimento não garanta, por si só, a adopção de comportamentos adequados (Bulgurcu et al., 2010; Herath & Rao, 2009).

Na dimensão da não conformidade, a figura contempla níveis como ignorância, apatia, negligência, resistência e violação deliberada. Estes níveis não devem ser interpretados como categorias universalmente estabelecidas, mas como uma representação analítica de diferentes formas e graus de comportamento de risco. Enquanto a ignorância ou a negligência podem estar associadas à falta de conhecimento, atenção ou capacidade para aplicar correctamente os procedimentos, a resistência e a violação deliberada podem envolver decisões conscientes de não cumprir as políticas organizacionais (Guo, 2013; Vance et al., 2012).

A utilidade desta representação reside, sobretudo, na possibilidade de relacionar diferentes comportamentos com estratégias de intervenção diferenciadas. Situações de desconhecimento, apatia ou negligência podem ser enfrentadas através de formação, sensibilização, comunicação e simplificação dos procedimentos. Por sua vez, comportamentos de resistência ou violação deliberada podem exigir mecanismos de supervisão, controlo e responsabilização, articulados com políticas claras e proporcionais (Herath & Rao, 2009; Bulgurcu et al., 2010).

A posição dos utilizadores neste continuum é influenciada por factores individuais e organizacionais. Entre os factores organizacionais destacam-se a cultura de segurança, a liderança, a clareza das políticas, a formação, a comunicação institucional e os mecanismos de acompanhamento e controlo. Uma cultura de segurança consistente pode favorecer a interiorização das práticas de protecção da informação, enquanto discrepâncias entre as políticas formais e as práticas quotidianas podem enfraquecer a sua credibilidade e reduzir a conformidade dos utilizadores (Da Veiga & Eloff, 2010; AlHogail, 2015; Glaspie & Karwowski, 2018).

Deste modo, a Figura 1 reforça a compreensão da segurança da informação como um fenómeno sociotécnico, resultante da interacção entre factores humanos, organizacionais e tecnológicos. Os utilizadores finais podem constituir fontes de vulnerabilidade, mas também agentes activos de protecção, dependendo das suas competências, motivações, comportamentos e condições organizacionais (Guo, 2013; Safa et al., 2015).

Em síntese, a representação conceptual evidencia que a segurança da informação não deve ser reduzida à implementação de mecanismos técnicos. A sua eficácia depende também da capacidade da organização para promover consciência, conformidade, comprometimento e uma cultura de segurança que favoreça a adopção de práticas seguras no quotidiano. Assim, as organizações devem procurar aproximar as políticas formais das práticas efectivamente observadas, articulando tecnologia, gestão, cultura organizacional e comportamento dos utilizadores.

1 DISCUSSÃO DE RESULTADOS

Os resultados da análise evidenciam que a segurança da informação deve ser compreendida como um fenómeno complexo, multidimensional e sociotécnico, no qual os factores humanos assumem um papel central. A literatura demonstra que abordagens predominantemente tecnológicas são insuficientes para responder à complexidade dos riscos actuais, uma vez que a eficácia dos mecanismos de protecção depende também da forma como os utilizadores compreendem e aplicam as práticas de segurança no contexto organizacional. Assim, o comportamento humano constitui parte integrante da segurança dos sistemas de informação (Furnell & Rajendran, 2012; Guo, 2013).

Os estudos analisados reforçam a relevância dos factores humanos na ocorrência, prevenção e mitigação de incidentes. A persistência de ameaças como *phishing*, engenharia social, comprometimento de credenciais e incumprimento de políticas demonstra que os riscos não podem ser explicados exclusivamente por vulnerabilidades técnicas. A consciência de segurança, a percepção do risco, a conformidade, os hábitos dos utilizadores e a cultura organizacional constituem igualmente dimensões relevantes para a protecção dos activos de informação (Bulgurcu et al., 2010; Safa et al., 2015). Relatórios recentes de ciber-segurança

mantêm igualmente o factor humano entre as dimensões críticas da exposição organizacional a incidentes (ENISA, 2024; IBM Security, 2024; Verizon, 2024).

Importa salientar que o presente estudo não envolveu recolha de dados empíricos primários. Por conseguinte, os exemplos de *phishing*, utilização indevida de credenciais, negligência ou incumprimento de políticas são apresentados como situações documentadas na literatura, e não como resultados produzidos directamente pela investigação. Esta distinção é metodologicamente necessária para evitar generalizações indevidas. Ainda assim, os modelos analisados apresentam aplicabilidade prática, ao permitirem compreender a interacção entre decisões individuais, práticas organizacionais e vulnerabilidades técnicas na produção de riscos de segurança (Ghafir et al., 2018; Glaspie & Karwowski, 2018).

A literatura evidencia, igualmente, que a protecção dos activos informacionais requer a articulação entre controlos técnicos, políticas institucionais, formação, comunicação, liderança e comportamentos dos utilizadores. A conformidade não depende apenas da existência de regras formais, mas também da percepção dos riscos, da utilidade das medidas de segurança, das normas sociais e das consequências associadas ao incumprimento (Herath & Rao, 2009; Bulgurcu et al., 2010). Deste modo, políticas tecnicamente adequadas podem produzir resultados limitados quando são pouco compreendidas, excessivamente complexas ou inadequadamente integradas nos processos de trabalho.

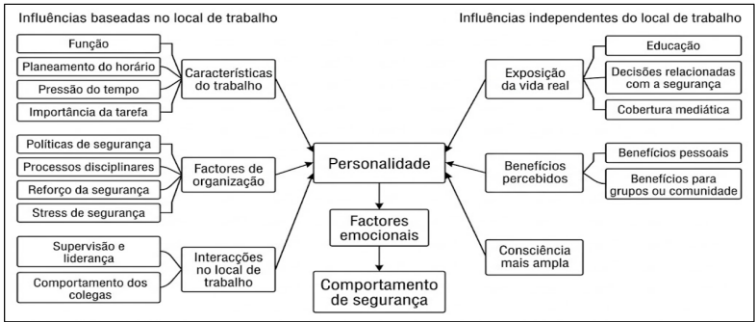
Apesar da sua utilidade, os modelos conceptuais apresentam limitações. A classificação dos comportamentos em categorias como conformidade, negligência, resistência ou violação deliberada pode simplificar uma realidade dinâmica, pois o mesmo utilizador pode adoptar comportamentos seguros ou de risco em função da pressão temporal, complexidade da tarefa, clareza das políticas, formação e percepção das consequências (Guo, 2013; Vance et al., 2012). Além disso, diferenças entre sectores, dimensões organizacionais, maturidade tecnológica e contextos culturais dificultam a generalização dos modelos. A cultura de segurança resulta da interacção entre valores, práticas, políticas e comportamentos organizacionais (Da Veiga & Eloff, 2010; AlHogail, 2015).

A análise permite ainda concluir que o comportamento inseguro não deve ser atribuído exclusivamente ao indivíduo. Políticas pouco claras, formação insuficiente, comunicação inadequada, liderança pouco envolvida, processos complexos e culturas permissivas podem favorecer práticas de risco (Safa et al., 2015; Glaspie & Karwowski, 2018). Ao nível individual, factores como conhecimento, percepção do risco, motivação, hábitos e consciência de segurança influenciam as decisões, embora o conhecimento, por si só, não garanta comportamentos seguros (McCormac et al., 2017; Ögütçü et al., 2016).

Em síntese, a segurança da informação exige uma abordagem integrada, articulando tecnologia, comportamento individual e contexto organizacional. Os modelos conceptuais são úteis para estruturar a análise, mas devem ser complementados por estudos empíricos e análises sectoriais. Consequentemente, estratégias eficazes de segurança devem combinar mecanismos técnicos com formação contínua, sensibilização, políticas claras, liderança, comunicação, responsabilização e desenvolvimento de uma cultura organizacional orientada para a segurança.

Figura 2

Modelo mediado psicossocial de formação de comportamento de segurança

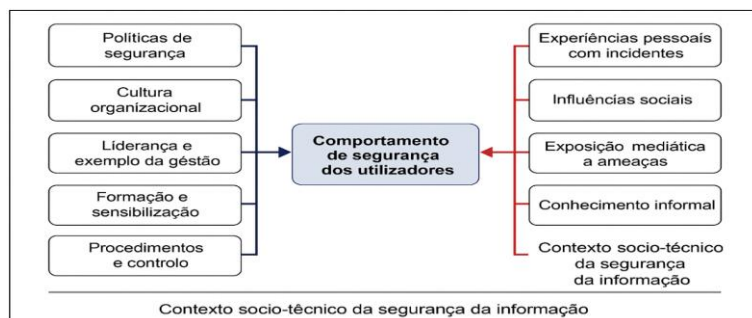


Fonte: Adaptado de Da Veiga e Eloff (2010), AlHogail (2015), Safa et al. (2015) e Glaspie & Karwowski (2018).

A Figura 2 apresenta um modelo conceptual das influências comportamentais na segurança da informação, segundo o qual o comportamento dos utilizadores resulta da interacção entre características individuais, factores organizacionais e influências externas. O modelo considera, por um lado, elementos relacionados com o contexto laboral, como as características da função, as políticas e práticas organizacionais, as relações interpessoais e as condições de trabalho; por outro, contempla influências externas, incluindo experiências pessoais, exposição a incidentes, interacções sociais e contacto com informação sobre segurança. Esta perspectiva é coerente com a literatura, que caracteriza o comportamento de segurança como resultado da combinação de factores individuais e contextuais (Guo, 2013; Safa et al., 2015).

Figura 3

Modelo de influências comportamentais na segurança de informação



Fonte: Elaboração própria, com base em Da Veiga e Eloff (2010) e AlHogail (2015).

Ao nível individual, as características de personalidade podem contribuir para explicar diferenças na percepção dos riscos, na interpretação das políticas e na adopção de comportamentos de protecção. Shropshire et al. (2015) evidenciam que determinados traços de personalidade, nomeadamente a conscienciosidade e a amabilidade, podem estar associados às intenções e à adopção de comportamentos relacionados com a segurança. Contudo, estas relações não devem ser interpretadas de forma determinística, uma vez que o comportamento efectivo resulta igualmente da interacção entre atitudes, percepções, condições organizacionais e características das tarefas. A consciência de segurança, a experiência, as normas sociais, a avaliação das ameaças e a auto-eficácia constituem igualmente factores relevantes (Safa et al., 2015).

Importa salientar que a Figura 3 constitui uma representação conceptual e não uma estrutura causal universalmente validada. As influências organizacionais e externas podem actuar através de mecanismos psicológicos, cognitivos e comportamentais, mas também exercer efeitos relativamente directos sobre as práticas dos utilizadores. Políticas claras, formação, mecanismos de controlo, normas organizacionais e procedimentos de trabalho podem condicionar as decisões individuais, enquanto experiências anteriores e influências sociais podem modificar percepções e atitudes perante o risco (Guo, 2013; Ng et al., 2009). Esta abordagem permite compreender o comportamento de segurança como dinâmico e dependente do contexto.

No plano organizacional, a cultura de segurança, a liderança, as políticas institucionais e as práticas de gestão constituem factores relevantes para a adopção de comportamentos seguros. Políticas claras, formação adequada, comunicação consistente e envolvimento da gestão podem favorecer a conformidade, enquanto discrepâncias entre normas formais e práticas efectivas podem reduzir a credibilidade das iniciativas de segurança (Da Veiga & Eloff, 2010; AlHogail, 2015; Safa et al., 2015). Assim, a segurança deve ser entendida como uma responsabilidade partilhada entre indivíduos e organização.

Os comportamentos de segurança também ultrapassam o contexto estritamente laboral. Experiências anteriores, conhecimentos adquiridos, interacções sociais e exposição a informação sobre ciber-segurança podem influenciar as atitudes e percepções dos utilizadores. Consequentemente, indivíduos submetidos às mesmas condições organizacionais podem adoptar comportamentos distintos, enquanto pessoas com características diferentes podem apresentar comportamentos semelhantes quando sujeitas a normas e condições contextuais equivalentes (Ng et al., 2009; Shropshire et al., 2015).

Do ponto de vista prático, as estratégias de segurança devem combinar mecanismos tecnológicos com intervenções dirigidas aos factores humanos. Sensibilização, formação adequada às funções, comunicação das políticas e promoção de boas práticas podem reduzir comportamentos de risco. Contudo, estas medidas devem ser articuladas com políticas compreensíveis, procedimentos exequíveis, supervisão e soluções tecnológicas orientadas para a usabilidade, uma vez que controlos excessivamente complexos podem favorecer comportamentos de contorno ou incumprimento (Furnell & Rajendran, 2012; Guo, 2013).

Em síntese, a Figura 2 reforça a compreensão da segurança da informação como fenómeno sociotécnico e psicossocial, no qual o comportamento dos utilizadores resulta da interacção entre factores individuais, organizacionais e externos (Fig. 3). Os factores humanos não constituem apenas uma fonte de vulnerabilidade, mas também um recurso estratégico para a protecção da informação. A eficácia das medidas de segurança depende, por conseguinte, da integração coerente entre tecnologia, processos, políticas, cultura e comportamento humano.

2 CONCLUSÃO

A segurança da informação constitui uma dimensão estratégica para organizações e sociedade, sobretudo perante a crescente digitalização e diversificação das ameaças cibernéticas. O estudo permitiu concluir que, embora os mecanismos técnicos sejam indispensáveis, a sua eficácia depende também da forma como os utilizadores interpretam as políticas e adoptam práticas seguras no quotidiano.

O estudo analisou o papel dos factores humanos na segurança da informação, considerando dimensões individuais, organizacionais e contextuais. A revisão da literatura demonstrou que os utilizadores podem representar simultaneamente uma vulnerabilidade e um recurso estratégico. Consciência de segurança, percepção de risco, experiência, atitudes, normas sociais e características individuais interagem com cultura de segurança, liderança, políticas internas, formação e práticas de gestão.

Conclui-se que uma abordagem exclusivamente tecnológica é insuficiente para responder de forma sustentável aos desafios da segurança da informação. A protecção efectiva requer articulação entre controlos técnicos, políticas organizacionais e comportamentos humanos, destacando-se a formação contínua, a sensibilização, a comunicação das políticas, o envolvimento da gestão e uma cultura organizacional favorável a práticas seguras.

O principal contributo consiste na sistematização integrada dos factores humanos, permitindo compreender o utilizador não apenas como potencial elo de vulnerabilidade, mas também como agente activo da segurança organizacional. Assim, a segurança da informação deve ser entendida como um fenómeno sociotécnico, no qual tecnologia, pessoas, processos e contexto institucional permanecem interligados.

Do ponto de vista prático, recomenda-se a implementação de programas contínuos de formação e sensibilização, políticas claras, mecanismos de acompanhamento e medidas ajustadas às funções desempenhadas. Os controlos técnicos devem igualmente considerar as práticas reais dos utilizadores, evitando procedimentos excessivamente complexos que possam favorecer o seu incumprimento.

Por fim, a natureza conceptual do estudo e a ausência de dados empíricos primários constituem limitações. Investigações futuras deverão testar as relações identificadas em diferentes sectores, organizações e perfis de utilizadores, aprofundando os mecanismos associados ao comportamento seguro e contribuindo para estratégias de segurança mais eficazes, sustentáveis e centradas nas pessoas.

3 TRABALHOS FUTUROS

Os resultados deste estudo evidenciam a necessidade de aprofundar empiricamente o papel dos factores humanos na segurança da informação. Estudos futuros deverão testar as relações identificadas em contextos organizacionais concretos, considerando a interacção entre características individuais, factores organizacionais, cultura de segurança e comportamentos dos utilizadores.

Uma primeira linha deverá privilegiar **estudos longitudinais**, mediante questionários aplicados em diferentes momentos, permitindo acompanhar a evolução da consciência de segurança, percepção de risco e comportamentos de conformidade. Assim, será possível avaliar os efeitos duradouros de programas de formação, campanhas de sensibilização e alterações das políticas internas.

Outra possibilidade consiste na realização de **estudos comparativos** entre organizações e sectores, como administração pública, banca, telecomunicações, ensino superior e saúde. Estes estudos poderão analisar a influência da cultura organizacional, maturidade tecnológica, liderança, políticas internas e mecanismos de controlo na adopção de práticas seguras, considerando diferenças contextuais.

A investigação futura deverá também aprofundar a **dimensão qualitativa**, recorrendo a entrevistas semiestruturadas com gestores, responsáveis de segurança, auditores e utilizadores finais. Esta abordagem permitirá compreender as razões associadas ao cumprimento, negligência ou resistência às normas, bem como as diferenças entre políticas formais e práticas quotidianas.

Será igualmente pertinente desenvolver **estudos experimentais ou quase-experimentais** para comparar estratégias de formação e sensibilização, incluindo simulações de *phishing*, gamificação, mensagens personalizadas e mecanismos de reforço. A utilização de métodos mistos, integrando questionários, entrevistas, análise documental e observação, permitirá obter evidências quantitativas e qualitativas mais abrangentes.

Em síntese, os trabalhos futuros deverão ultrapassar modelos conceptuais e produzir evidências empíricas robustas sobre os factores associados ao comportamento seguro, as condições em que actuam e os mecanismos através dos quais produzem efeitos. Tal orientação poderá contribuir para estratégias de segurança mais eficazes, contextualizadas, sustentáveis e centradas nas pessoas.

4 REFERÊNCIAS BIBLIOGRÁFICAS

- Albladi, S. M., & Weir, G. R. S. (2018). User characteristics that influence judgment of social engineering attacks in social networks. *Human-Centric Computing and Information Sciences*, 8, Article 5. <https://doi.org/10.1186/s13673-018-0128-7>
- AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, 49, 567–575. <https://doi.org/10.1016/j.chb.2015.03.054>
- Alshaikh, M. (2021). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, 98, 102003. <https://doi.org/10.1016/j.cose.2020.102003>
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523–548. <https://doi.org/10.2307/25750690>
- Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, 29(2), 196–207. <https://doi.org/10.1016/j.cose.2009.09.002>
- Delso-Vicente, A.-T., Diaz-Marcos, L., Aguado-Tevar, O., & García de Blanes-Sebastián, M. (2025). Factors influencing employee compliance with information security policies: A systematic literature review of behavioral and technological aspects in cybersecurity. *Future Business Journal*, 11, Article 28. <https://doi.org/10.1186/s43093-025-00452-7>
- ENISA. (2024). *ENISA threat landscape 2024*. European Union Agency for Cybersecurity. <https://www.enisa.europa.eu>
- Flores, W. R., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, 43, 90–110. <https://doi.org/10.1016/j.cose.2014.03.004>
- Furnell, S., & Rajendran, A. (2012). Understanding the influences on information security behaviour. *Computer Fraud & Security*, 2012(3), 12–15. [https://doi.org/10.1016/S1361-3723\(12\)70053-2](https://doi.org/10.1016/S1361-3723(12)70053-2)
- Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., & Baker, T. (2018). Security threats to critical infrastructure: The human factor. *The Journal of Supercomputing*, 74, 4986–5002. <https://doi.org/10.1007/s11227-018-2337-2>

- Glaspie, H. W., & Karwowski, W. (2018). Human factors in information security culture: A literature review. In T. Ahram & W. Karwowski (Eds.), *Advances in human factors in cybersecurity* (pp. 267–280). Springer. https://doi.org/10.1007/978-3-319-60585-2_25
- Grant, M. J., & Booth, A. (2009). A typology of reviews: An analysis of 14 review types and associated methodologies. *Health Information & Libraries Journal*, 26(2), 91–108. <https://doi.org/10.1111/j.1471-1842.2009.00848.x>
- Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security*, 32, 242–251. <https://doi.org/10.1016/j.cose.2012.10.003>
- Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106–125. <https://doi.org/10.1057/ejis.2009.6>
- IBM Security. (2024). *Cost of a data breach report 2024*. IBM. <https://www.ibm.com/reports/data-breach>
- Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: An interdisciplinary review and framework proposal. *International Journal of Information Security*. <https://doi.org/10.1007/s10207-025-01032-0>
- Luo, X., & Zhang, D. (2017). Special issue introduction: A comprehensive perspective on information systems security—Technical advances and behavioral issues. *Decision Support Systems*, 100, 1–2. <https://doi.org/10.1016/j.dss.2017.05.001>
- McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, 69, 151–156. <https://doi.org/10.1016/j.chb.2016.11.065>
- Ng, B.-Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, 46(4), 815–825. <https://doi.org/10.1016/j.dss.2008.11.010>
- Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, 56, 83–93. <https://doi.org/10.1016/j.cose.2015.10.002>
- Pimenta, A. M., Silva, S. C., & Figueiredo, R. Q. (2016). A segurança dos sistemas de informação e o comportamento dos usuários. *Journal of Information Systems and Technology Management*, 13(3), 533–552. <https://doi.org/10.4301/S1807-17752016000300007>
- Renaud, K., Ophoff, J., von Solms, R., & Dlamini, M. (2022). Human and contextual factors influencing cyber-security in organizations, and implications for higher education institutions: A systematic review. *Global Knowledge, Memory and Communication*, 73(12), 1–23. <https://doi.org/10.1108/GKMC-12-2021-0209>
- Safa, N. S., Sookhak, M., von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, 53, 65–78. <https://doi.org/10.1016/j.cose.2015.05.012>
- Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, 49, 177–191. <https://doi.org/10.1016/j.cose.2015.01.002>
- Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339. <https://doi.org/10.1016/j.jbusres.2019.07.039>
- Sutton, A., & Tompson, L. (2025). Towards a cybersecurity culture-behaviour framework: A rapid evidence review. *Computers & Security*, 148, 104110. <https://doi.org/10.1016/j.cose.2024.104110>
- Torten, R., & Reaiche, C. (2018). The impact of security awareness on information technology professionals' behavior. *Computers & Security*, 79, 8–20. <https://doi.org/10.1016/j.cose.2018.08.010>
- Vance, A., Siponen, M., & Pahnla, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, 49(3–4), 190–198. <https://doi.org/10.1016/j.im.2012.04.002>
- Verizon. (2024). *2024 data breach investigations report*. Verizon. <https://www.verizon.com/business/resources/reports/dbir/>