

Erro humano

Um risco amplamente subestimado na tecnologia de transformação digital

Não devem restar dúvidas de que a transformação digital é uma necessidade organizacional realizada com o objetivo de manter, sustentar e aprimorar a relevância de uma empresa para seus constituintes. Mais especificamente, a relevância pode abranger tudo: desde atrair clientes no setor privado até aumentar a conveniência e o acesso aos serviços do governo pelos cidadãos.

Embora tenha havido um forte foco no aspecto "digital" da transformação digital, a conversa traz cada vez mais uma visão mais inclusiva do impacto da transformação digital em uma empresa: seus clientes, modelo operacional e modelo de negócios.¹

A conscientização dos extensos fatores humanos de risco existentes na transformação digital precisa ser aprimorada.

Visão geral das tecnologias de transformação digital

De todas as tecnologias emergentes no mercado, várias delas foram identificadas como mais propensas a mudar a maneira como as organizações fazem negócios.² Diante da natureza dinâmica do desenvolvimento tecnológico, esta lista está sujeita a alterações, mas há várias tecnologias que são mais relevantes hoje.

Drones

Os drones, ou veículos aéreos não tripulados (UAVs), foram originalmente criados para fins militares.³ Eles representam uma convergência de várias tecnologias, incluindo robótica, inteligência artificial (IA) e aeronáutica.

Em 2013, acreditava-se que uma das razões para o elevado número de acidentes com drones fosse a variedade de interfaces de controle usadas para pilotar os veículos, resultando na criação do Instituto Nacional Americano de Padrões/Sociedade de Fatores Humanos e Ergonomia (ANSI/HFES) 100-2007, com o objetivo de padronizar a interface de controle.⁴ No entanto, em 2016, a tecnologia foi citada como a principal causa de acidentes com drones, especificamente a perda de sinal

entre o operador e o drone.⁵ Em um contexto militar, os drones estão sujeitos a erros humanos e podem ter um impacto negativo na vida civil.⁶

Robótica

A robótica também é uma convergência de tecnologias, incluindo engenharia mecânica, engenharia eletrônica e ciência da computação.

A palavra "robô" é derivada da palavra tcheca *robota*, que significa servo ou "trabalhador".⁷ Os robôs precisam de uma programação robusta para serem totalmente produtivos e, nesse ponto, os humanos ainda têm a tarefa de programar. Apesar das habilidades certas e da devida diligência, os erros humanos de codificação podem acontecer, interrompendo o fluxo de trabalho e a produção enquanto os códigos são depurados, o que pode custar tempo e dinheiro significativos às empresas.⁸ A manutenção incorreta ou incorreta pode



Guy Pearce, CGEIT

É o diretor-chefe de transformação digital da Convergence. Ele também atuou em conselhos de governança nas áreas de serviços bancários e financeiros em uma organização sem fins lucrativos e como diretor de segurança da informação de uma organização de serviços financeiros. Pearce tem mais de uma década de experiência em governança de dados e governança de TI e criou um curso de Transformação Digital para a SCS da Universidade de Toronto (Ontário, Canadá). Ele recebeu o Prêmio de Melhor Autor Michael Cangemi ISACA® 2019 por contribuições para o campo da governança de TI.

“A IA É PROGRAMADA POR HUMANOS E, NOVAMENTE, É EXATAMENTE ONDE ESTÃO OS PROBLEMAS QUE PODEM GERAR RISCOS.”

resultar em um robô com defeito, o que pode também pode custar caro.⁹

Blockchain

Embora a tecnologia blockchain tenha ido além do esperado em 2018, existem organizações que estão usando blockchain para resolver problemas reais de negócios, como a produção sustentável de casimira na Mongólia.¹⁰

Embora os erros na blockchain sejam raros, o ponto da interface entre a blockchain e outros sites, interfaces e plataformas é onde o erro humano pode ocorrer, e isso precisa ser resolvido por uma formação mais aprofundada do desenvolvedor.¹¹ Além disso, é importante lembrar que, quando o blockchain é usado como um banco de dados, essas informações estão sujeitas às mesmas deficiências humanas que qualquer outro banco de dados.¹² O Risco de integração e a vulnerabilidade de software são os maiores fatores de risco humano nessa tecnologia.¹³

Impressão 3D

Com a impressão 3D, os objetos tridimensionais são criados camada por camada, usando uma ampla gama de materiais, em vez de serem criados por artesãos qualificados e precisos. Essa tecnologia é usada na fabricação, onde o erro humano é um fator maior do que em outros setores.¹⁴

Como em outras tecnologias emergentes, a falta de especialização e os requisitos de desenvolvimento de software associados à impressão 3D¹⁵ ainda apresentam risco humano associado à tecnologia. Embora ainda existam desafios com o uso da impressão 3D na área da saúde,¹⁶ erros causados por humanos neste setor também podem ter consequências éticas.

Internet das Coisas e Internet das Coisas Industrial

As velocidades mais rápidas da Internet com larguras de banda superiores levaram a uma proliferação de dispositivos que podem se comunicar com um dispositivo central ou com outros aparelhos. Essa

tendência vai ser acelerada com a adoção do 5G. Embora um smartphone possa ser considerado um tipo de dispositivo da Internet das Coisas (IoT) com recursos como um sistema de posicionamento global (GPS) e um acelerômetro de três eixos, a Internet das Coisas Industrial (IIoT) envolve explicitamente sensores robustos, de baixa potência (remotos) e nível industrial.

Novamente, os fatores de risco humanos na IoT e IIoT estão relacionados à programação e ao design de hardware dos dispositivos IoT e IIoT.¹⁷ Além disso, esses dispositivos são geralmente fabricados por robôs, que têm seus próprios desafios humanos (como mencionado anteriormente), levando a uma cascata de fatores de risco humanos. Um dos maiores fatores de risco humano, porém, é encontrado na segurança cibernética¹⁸ e as pessoas são reconhecidas como "o elo mais fraco da segurança da informação".¹⁹

IA

Máquinas pensantes autônomas fascinam o imaginário humano há anos, levando a histórias assustadoras sobre um mundo governado por robôs inteligentes. No entanto, como a sociedade digital de hoje se baseia em software vulnerável a falhas de programação e ataques cibernéticos, essa singularidade - o ponto em que a IA ultrapassa a inteligência humana - é altamente improvável.²⁰

A IA é programada por humanos e, mais uma vez, é exatamente onde estão os problemas que podem gerar riscos. A IA é empregada em drones, robôs e dispositivos de IoT e IIoT. Os erros humanos são, portanto, amplificados e somados aos erros que ocorrem na tecnologia integrada. No entanto, há um risco mais sutil associado à IA, que decorre do fato de que a IA está repleta de preconceitos humanos.²¹ Como a IA precisa de seres humanos para validar seus resultados,²² pelo menos inicialmente, o erro humano pode surgir para impactar os resultados. Outra questão é a qualidade dos dados usados para treinar sistemas de IA. Com base na experiência, a qualidade dos dados quase nunca é tão boa quanto o necessário.

Realidade aumentada/Realidade virtual

Em certo sentido, a realidade virtual (VR) é um espelho digital da realidade que ela modela. A realidade aumentada (RA), por outro lado, contribui para a experiência da RV. Por exemplo, o Google Lens fornece informações adicionais sobre a realidade física com a qual estamos interagindo.

Novamente, os sensores coletam informações e sua interpretação é determinada pela programação. Da mesma forma, a qualidade do acréscimo é determinada pela qualidade da programação. Se algo observado na realidade física não estiver no "dicionário" da RV, ele pode não ser descrito como pretendido na versão virtual. Portanto, a qualidade da experiência de RA/VR depende da qualidade dos dados que recebe por meio dos sensores relevantes e dos dados usados para criar o modelo para o mecanismo de reconhecimento, sendo que este último pode ser negativamente influenciado por deficiências humanas durante modelagem e programação.

Próximo nível de tecnologias saindo do forno

As principais novas tecnologias continuarão a mudar a maneira como os negócios são conduzidos. A tecnologia em nuvem já está aqui e outras como 5G, computação sem servidor e biometria devem ser consideradas. Novamente, cada tecnologia emergente envolve fatores de risco humano que valem a pena ser analisados como parte de uma estratégia diligente de transformação digital.

Fatores de risco humano

Com base na discussão anterior, os elementos de risco humano comuns em todas as tecnologias de transformação digital podem ser vinculados à programação, design e dados. Em outras palavras, os mesmos esforços humanos que produzem tecnologias de transformação digital são os mesmos que os colocam em risco.

Para estender a análise, o risco de TI pode ser considerado em sete subdisciplinas: segurança cibernética, resiliência, fornecedores e terceiros, projetos e mudanças, ciclo de vida de desenvolvimento de software (SDLC), dados e compliance.²³ O termo SDLC refere-se ao processo de produção de software, seja ágil ou em sequência; que se inicia com a aprovação da arquitetura e termina com a implantação e manutenção. Cada uma dessas subdisciplinas possui componentes de risco humano:

1. Segurança cibernética—"O combate às ameaças cibernéticas requer foco nas pessoas e nos comportamentos, não apenas na tecnologia".²⁴

2. Resiliência—"O risco humano é negligenciado nos planos de recuperação de desastres".²⁵

“ERROS HUMANOS NA CAPTURA DE DADOS, TRANSFORMAÇÃO DE DADOS E MIGRAÇÃO DE DADOS SÃO TÃO ANTIGOS QUANTO O PRÓPRIO COMPUTADOR.”

3. Fornecedores—A realização de “due-dilligences” em fornecedores é um esforço com grande trabalho humano, e erros podem acontecer.

4. Projetos—O gerenciamento de mudanças faz parte de uma implantação bem-sucedida e, na maioria das vezes, exige adequações no comportamento humano para garantir resultados desejáveis.

5. SDLC—Os seres humanos avaliam as implicações arquitetônicas de uma nova tecnologia, projetam os programas (e dispositivos), criam os programas e, em grande medida, os testam, especialmente em implantações complexas. Onde quer que os humanos estejam envolvidos, é provável que erros ocorram

6. Dados—Erros humanos na captura, transformação e migração de dados são tão antigos quanto o próprio computador.

7. Compliance—Muitos requisitos de compliance são atendidos por um conjunto de regras, mas alguns estão abertos a interpretações. Pode ser da natureza humana que a interpretação erre à favor da organização, e não em termos do espírito da legislação.

Ao avaliar o risco relacionado à tecnologia de transformação digital de uma organização, pode ser significativo criar uma tabela resumindo as áreas de risco relevantes e capturar os detalhes de cada célula em uma estrutura típica de gerenciamento de riscos (por exemplo, identificar, analisar, avaliar, controlar, monitorar, gerar relatórios). A **Figura 1** ilustra os elementos de risco humano (X) na interseção das sete subdisciplinas de risco de TI e as tecnologias de transformação digital mais significativas previamente identificadas. As células em rosa escuro representam os tópicos discutidos no texto. A interpretação desses domínios de risco depende dos perfis de risco incrementais das implantações específicas das tecnologias de transformação digital.

Figura 1 - Elementos de risco humano baseados no risco de TI nas tecnologias de transformação digital								
		Tecnologias de Transformação Digital						
		Drones	Robótica	Blockchain	Impressão 3D	IoT e IIoT	IA	RA/RV
Subdisciplinas de Risco de TI	Segurança cibernética					X		
	Resiliência		X		X	X		
	Fornecedores	X	X	X	X	X	X	X
	Projetos	X	X	X	X	X	X	X
	SDLC	X	X	X	X	X	X	X
	Dados	X	X	X	X	X	X	X
	Conformidade	X	X					

Na **figura 1**, podemos observar que a resiliência é especialmente relevante para a robótica e a IoT/IIoT, dada a alta criticidade dessas tecnologias para o setor de fabricação. De maneira geral há um impacto nos fornecedores, projetos, SDLC e subdisciplinas de dados, especialmente em grandes organizações. Particularmente, a categoria de dados envolve um risco humano de entrada e um risco de saída: que se refere ao risco humano relacionado à análise, interpretação e ação sobre os dados produzidos por uma tecnologia de transformação digital. Na categoria compliance, além da ANSI/HFES 100-2007, a norma de qualidade ISO 9000 da Organização Internacional para Padronização (ISO) é importante para a fabricação na qual a robótica desempenha um papel.

Adotar medidas para reduzir o erro humano

As auditorias de TI se concentram tradicionalmente nos recursos ao considerar o risco da tecnologia, mas, partindo da análise anterior, fica claro que as implicações (humanas) dos recursos são muito mais significativas do que se pensava anteriormente. Como resultado, o objetivo deve ser reduzir a incidência de erro humano. Existem três recursos que podem levar a uma redução no erro humano:²⁶

1. **Detectabilidade**—A capacidade de identificar erros e impedir que ocorram
2. **Rastreabilidade**—A capacidade de identificar a causa raiz do erro e instituir medidas corretivas
3. **Destreza**—A capacidade de executar uma tarefa sem incorrer em erros

Cada um desses recursos pode ser reforçado por uma cultura que apoie treinamentos e processos adequados.

A questão é se os custos incrementais necessários para implementar essas medidas são considerados válidos no contexto de mitigação dos custos potenciais de um erro.

Por fim, quaisquer que sejam as medidas adotadas para reduzir o erro humano, os auditores devem "manter um nível de ceticismo profissional suficiente ao revisar a avaliação de riscos da gerência para novos sistemas",²⁷ considerando as pessoas como um fator (causa) de risco, em vez de apenas relatar seus sintomas (por exemplo, código com bugs).

“AS AUDITORIAS DE TI SE CONCENTRAM TRADICIONALMENTE NOS RECURSOS AO CONSIDERAR O RISCO DE TECNOLOGIA, MAS, PARTINDO DA ANÁLISE ANTERIOR, FICA CLARO QUE AS IMPLICAÇÕES (HUMANAS) DOS RECURSOS SÃO MUITO MAIS SIGNIFICATIVAS DO QUE SE PENSAVA ANTERIORMENTE.”

Conclusão

A **Figura 1** ilustra que o elemento de risco humano está bastante enraizado na tecnologia de transformação digital. Ele está presente em cada uma das tecnologias de transformação digital discutidas neste artigo e em cada uma das subdisciplinas de risco de TI. A escala de risco humano na transformação digital é vasta e exige

um foco intenso nas pessoas e no comportamento (cultura), no esforço para implementar uma estratégia bem-sucedida de transformação digital, incluindo mecanismos que se concentram explicitamente na redução da incidência de erro humano.

Vale ressaltar que o efeito em cascata do erro humano que ocorre quando o risco humano em uma tecnologia (por exemplo, IA) é introduzido em outra tecnologia que possui seus próprios elementos de risco humano (por exemplo, drones), o que significa que o gerenciamento de riscos se torna mais complexo. Medidas urgentes são necessárias a fim de garantir a sustentabilidade não apenas da nova tecnologia, mas também da organização que está implantando a nova tecnologia e também garantir o sucesso da estratégia de transformação digital.

Diante da escala dos elementos de risco humano identificados na tecnologia de transformação digital, deve ser óbvio que a mera realização de uma intervenção rápida de "gerenciamento de mudanças" após a implantação não será suficiente (parte da linha "Projetos" na **figura 1**). O fator humano faz parte de quase todos os elementos da transformação digital, o que significa que é necessária atenção especial para mitigar o risco associado e, finalmente, garantir o sucesso e a sustentabilidade da iniciativa de transformação digital.

Notas de rodapé

- 1 Pearce, G.; "Enhancing the Board's Readiness for Digital Transformation Governance," *ISACA® Journal*, vol. 5, 2019, <https://www.isaca.org/archives>
- 2 Pearce, G.; "Acknowledging Humanity in the Governance of Emerging Technology and Digital Transformation," *ISACA Journal*, vol. 4, 2019, <https://www.isaca.org/archives>
- 3 Vyas, K.; "A Brief History of Drones: The Remote Controlled Unmanned Aerial Vehicles (UAVs)," *Interesting Engineering*, 2 de janeiro de 2018, <https://interestingengineering.com/a-brief-history-of-drones-the-remote-controlled-unmanned-aerial-vehicles-uavs>
- 4 Atherton, K. D.; "What Causes So Many Drone Crashes?" *Popular Science*, 4 de março de 2013, <https://www.popsci.com/technology/article/2013-03/human-error-after-all/>
- 5 *Business Insider*, "Drone Accidents Are Due to Tech, Not Human Error," 25 de agosto de 2016, <https://www.businessinsider.com/drone-accidents-due-to-tech-not-human-error-2016-8>
- 6 King, T.; "Positive and Negative Effects of Drones," *Positive Negative Impact*, 8 de julho de 2019, <https://positivenegativeimpact.com/drones>
- 7 Hockstein, N. N.; C. G. Gourin; R. A. Faust; D. J. Terris; "A History of Robots: From Science Fiction to Surgical Robotics," *Journal of Robotic Surgery*, 17 de março de 2007, <https://link.springer.com/article/10.1007/s11701-007-0021-2>
- 8 Matthews, K.; "Four Reasons You Still Need to Watch for Human Error When Working With Robotics," *RobotIQ*, 22 de novembro de 2018, <https://blog.robotiq.com/4-reasons-you-still-need-to-watch-for-human-error-when-working-with-robotics>
- 9 *Ibid.*
- 10 Huang, R.; "UN Pilot in Mongolia Uses Blockchain to Help Farmers Deliver Sustainable Cashmere," *Forbes*, 28 de dezembro de 2019, <https://www.forbes.com/sites/rogerhuang/2019/12/28/un-pilot-in-mongolia-uses-blockchain-to-help-farmers-deliver-sustainable-cashmere/#60cedd8717d9>
- 11 Tanase, B.; "Human Error as a Limitation for Blockchain Adoption?" *Medium*, 21 de dezembro de 2017, <https://medium.com/@biancatanase/human-error-as-a-limitation-for-blockchain-adoption-80f3da30e8be>
- 12 Davies, C.; "Blockchain's Issues and Limitations," *Cryptoboom*, 9 de dezembro de 2017, <https://cryptoboom.com/basics/blockchain/blockchains-issues-and-limitations>



Gostou do artigo?

- Leia o artigo *O futuro da Auditoria de TI. Audit.* www.isaca.org/Future-of-IT-Audit
- Saiba mais, discuta e colabore sobre gerenciamento de riscos nos fóruns on-line da ISACA. <https://engage.isaca.org/onlineforums>



- 13 Raman, R.; M. Mangnaik; "Blockchain Can Transform the World, but Is It Fool-Proof?" *Huffington Post*, 24 de janeiro de 2017, https://www.huffingtonpost.in/raja-raman/blockchain-can-transform-the-world-but-is-it-fool-proof_a_21660586/
- 14 Wright, I.; "Human Error Is Worse in Manufacturing Compared to Other Sectors," *Engineering.com*, 8 de novembro de 2017, <https://www.engineering.com/Advanced-Manufacturing/ArticleID/15974/Human-Error-is-Worse-in-Manufacturing-Compared-to-Other-Sectors.aspx>
- 15 Tractus3D, "3D Printing for Manufacturing," <https://tractus3d.com/industries/3d-printing-for-manufacturing/>
- 16 Wright, C.; "3D Printing in Healthcare," PreScouter, abril de 2017, <https://www.prescouter.com/2017/04/3d-printing-healthcare/>
- 17 Joyce, J.; "How the Internet of Things Is Affecting Laboratory Equipment," *Lab Manager*, 7 de maio de 2018, <https://www.labmanager.com/laboratory-technology/2018/05/how-the-internet-of-things-is-affecting-laboratory-equipment>
- 18 *Ibid.*
- 19 Lineberry, S.; "The Human Element: The Weakest Link in Information Security," *Journal of Accountancy*, 1 de novembro de 2007, <https://www.journalofaccountancy.com/issues/2007/nov/thehumanelementtheweakestlinkininformationsecurity.html>
- 20 Thomas, M.; "Human Error, Not Artificial Intelligence, Poses the Greatest Threat," *The Guardian*, 3 de abril de 2019, <https://www.theguardian.com/technology/2019/apr/03/human-error-not-artificial-intelligence-poses-the-greatest-threat>
- 21 *Op cit* Pearce, "Acknowledging Humanity in the Governance of Emerging Technology and Digital Transformation"
- 22 Kent, J.; "Artificial Intelligence Success Requires Human Validation, Good Data," *Health IT Analytics*, 26 de novembro de 2019, <https://healthitanalytics.com/news/artificial-intelligence-success-requires-human-validation-good-data>
- 23 McKinsey & Company, "The Ghost in the Machine: Managing Technology Risk," julho de 2016, <https://www.mckinsey.com/business-functions/risk/our-insights/the-ghost-in-the-machine-managing-technology-risk>
- 24 Walker, E.; D. Witkowski; S. Benczik; P. Jarrin; "Cybersecurity—The Human Factor," Federal Information Systems Security Educator's Association, 2017, https://csrc.nist.gov/CSRC/media/Events/FISSEA-30th-Annual-Conference/documents/FISSEA2017_Witkowski_Benczik_Jarrin_Walker_Materials_Final.pdf
- 25 Ashford, W.; "Human Risk Is Neglected in Disaster Plans, Warns Study," *Computer Weekly*, 9 de novembro de 2007, <https://www.computerweekly.com/news/2240083858/Human-risk-is-neglected-in-disaster-plans-warns-study>
- 26 Nakata, T.; "Human Error Prevention," Slideshare, 19 de dezembro de 2011, <https://www.slideshare.net/torunakata/human-error-prevention>
- 27 Lindsay, J. B.; A. Doult; C. Ide; "Emerging Technologies, Risk, and the Auditor's Focus," Harvard Law School Forum on Corporate Governance, 8 de julho de 2019, <https://corpgov.law.harvard.edu/2019/07/08/emerging-technologies-risk-and-the-auditors-focus/>