IBRACON

Instituto de Auditoria Independente do Brasil

Cybersecurity

A importância para o mercado e para a Auditoria Independente

AGENDA

01. Responsabilidade da Auditoria Independente sobre Cybersecurity

02. Contexto Geral

03. Ações dos Reguladores

04. Frameworks da indústria

IBRACON
Instituto de Auditoria Independente do Brasil

Edson Honda - CISSP

Sócio em firma de auditoria associada – Cybersecurity & Privacy

EXPERIÊNCIA PROFESSIONAL

- Profissional com mais de 30 anos de experiência em TI e Cybersecurity:
  - Atuou em consultorias locais e globais, atendendo organizações na América Latina em projetos de Transformação, Riscos, Governança, Auditoria de Segurança Cibernética em clientes de diferentes setores / indústrias.
  - Foi CISO e de Gerente de Auditoria de Sistemas de TI em uma grande empresa de transportes aéreos
  - Foi professor na FIAP, responsável pela cadeira de Segurança de Redes no curso MBA de Segurança da Informação.

Educação, licenças e certificações

- CISSP – ISC2
- Pós-graduado pela FIAP (Faculdade de Informática e Administração Paulista) no curso MIT - Mestre em Tecnologia da Informação
- Graduado pela Fundação Santo André no curso Bacharel em Matemática com ênfase em Processamento de Dados

Rodrigo Gonza

Sócio em firma de auditoria associada – IT Audit

EXPERIÊNCIA PROFESSIONAL

- Profissional com mais de 20 anos de experiência em auditoria de tecnologia da informação:
  - Rodrigo lidera projetos de auditoria de sistemas em conexão com os trabalhos de auditoria de demonstrações financeiras e auditorias integradas (SOx).
  - Atuou também em projetos de auditoria interna de sistemas, controles internos, governança de TI, mapeamento e redesenho de processos, Sarbanes Oxley, segregação de funções e segurança da informação.
  - Atualmente é o sócio líder das práticas de IT Audit da KPMG no Brasil e Américas e do Audit Technology & Innovation, responsável pelas soluções digitais e de inovação para a prática de auditoria da KPMG no Brasil e América do Sul.

Educação, licenças e certificações

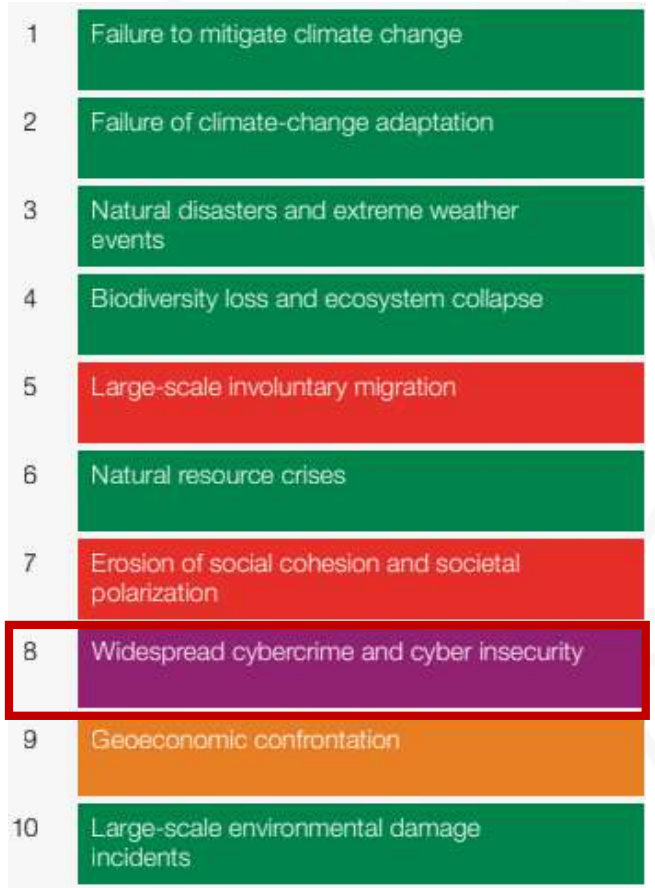
- Pós-graduado em Segurança de Sistemas e Ambientes Operacionais pela FASP.
- Graduado em Sistemas de Informação pela Faculdade de Tecnologia (FATEC).
- Certificado Cobit, ISO 27001 e Lotus Certified Professional.

IBRACON
Instituto de Auditoria Independente do Brasil

WEF – Global Risks Report 2023

Intervalo de 2 anos

Intervalo de 10 anos



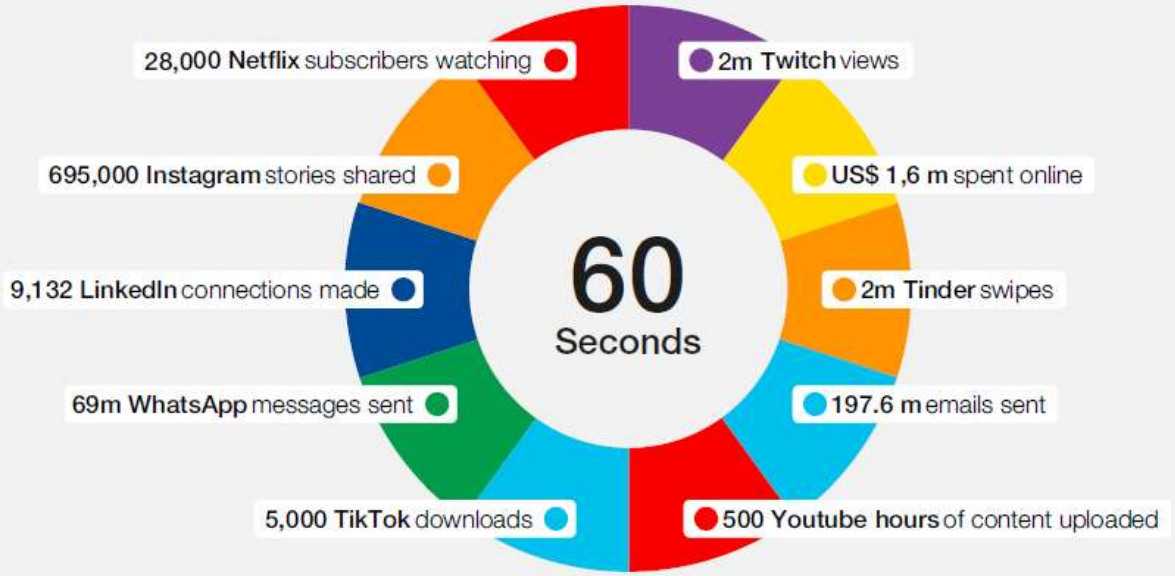
Economic | Environmental | Geopolitical | Societal | Technological

Fonte: World Economic Forum - The Global Risks - Report 2023 - 18th Edition - **Disponível em**: https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

IBRACON
Instituto de Auditoria Independente do Brasil

Dependências Digitais e Vulnerabilidades em Cyber

Quantidade estimada de dados criados na Internet em um minuto



800 bilhões

Estimativa do crescimento, em valores, do comércio digital até 2024

435%

Aumento de ataques de ransomware em 2020

3 milhões

Gap em profissionais de cybersecurity no mundo

95%

Dos problemas com cybersecurity atribuídos a erros humanos

Fonte: World Economic Forum - The Global Risks - Report 2022 - 17th Edition - **Disponível em**: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

IBRACON
Instituto de Auditoria Independente do Brasil

Custo do crime cibernético deve atingir um patamar anual de $10.5 Trilhões até 2025

CYBERCRIME MAGAZINE

ABOUT RESEARCH NEW

Cybercrime To Cost The World $10.5 Trillion Annually By 2025

Special Report: Cyberwarfare In The C-Suite.

– Steve Morgan, Editor-in-Chief

Sausalito, Calif. – Nov. 13, 2020

If it were measured as a country, then cybercrime — which is predicted to inflict damages totaling $6 trillion USD globally in 2021 — would be the world's third-largest economy after the U.S. and China.

Cybersecurity Ventures expects global cybercrime costs to grow by 15 percent per year over the next fi years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015. This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, is exponentially larger than the damage inflicted from natural disasters in a year, and will be more profitabl than the global trade of all major illegal drugs combined.

The damage cost estimation is based on historical cybercrime figures including recent year-over-year growth, a dramatic increase in hostile nation-state sponsored and organized crime gang hacking activitie and a cyberattack surface which will be an order of magnitude greater in 2025 than it is today.

Cybercrime costs include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm.

FORBES > INNOVATION

10.5 Trillion Reasons Why We Need A United Response To Cyber Risk

Forbes

Carmen Ene Forbes Cou
Forbes Technology Coun
COUNCIL POST | Membe

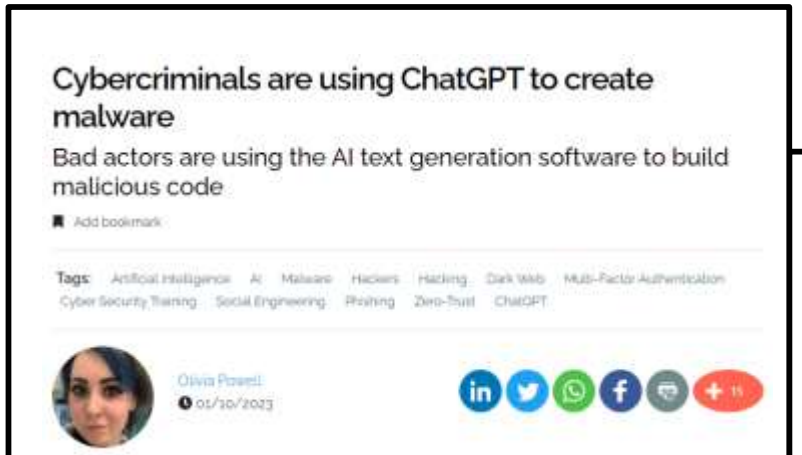
Carmen Ene is CEO at 3stepIT of Europe's leading circular te providers.

The Davos, Switzerland, resort was once again alive with activity in January as world leaders gathered to discuss how to tackle global challenges, with climate change once again at the top of the agenda. However, this year, another critical issue vied for the delegates' attention: cybersecurity. And for good reasons.

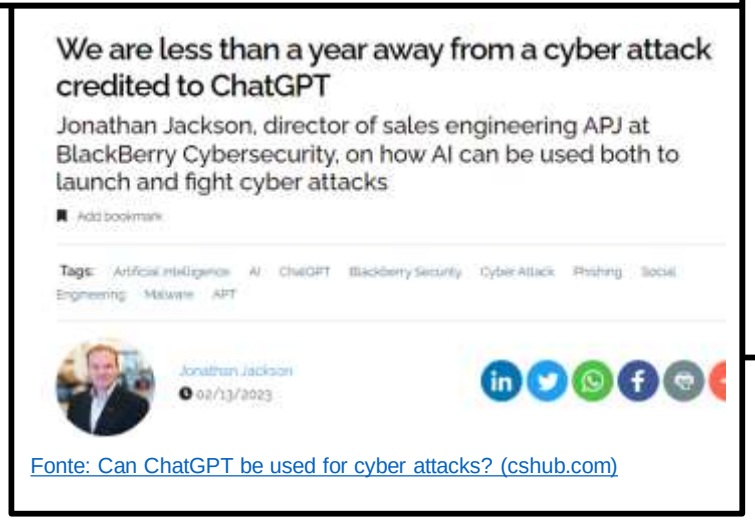
The 2023 World Economic Forum's (WEF) Global Risks Report, published in January, put cybersecurity in the current and future top 10 risks globally. The cost of cybercrime is projected to hit an annual $10.5 trillion by 2025, according to Cybersecurity Ventures. By the same token, Gartner analysts predict that over the next two years, 45% of global organizations will be impacted in some way by a supply chain attack.

IBRACON
Instituto de Auditoria Independente do Brasil

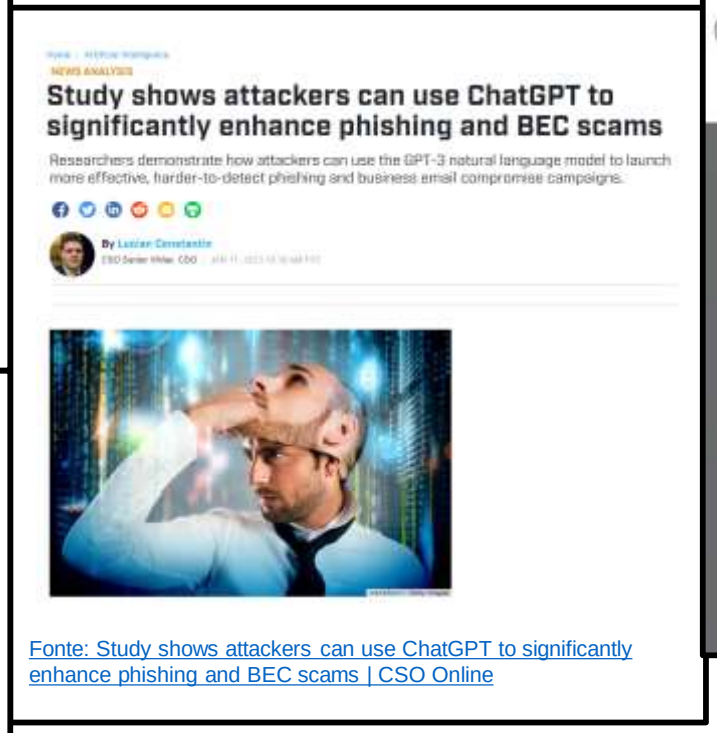
Tendências de Novos Riscos Cibernéticos



Fonte: Cybercriminals are using ChatGPT to create malware (cshub.com)



Fonte: Can ChatGPT be used for cyber attacks? (cshub.com)



Fonte: Study shows attackers can use ChatGPT to significantly enhance phishing and BEC scams | CSO Online

Fonte: Phishing via QR Code crescem quase 600%; como se proteger (uol.com.br)

IBRACON
Instituto de Auditoria Independente do Brasil

Ataque virtual à um dos maiores fornecedores mundiais e a empresa líder em serviços de relacionamento com clientes e terceirização de processos de negócios na América Latina custou US$ 46 mi

UOL - [A EMPRESA] foi vítima de um ataque virtual no ano passado e teve que desligar os servidores por vários dias. Qual foi o impacto?

[EXECUTIVO DA EMPRESA] O ciberataque é um problema endêmico no mundo. Existem empresas que, infelizmente, praticam estes atos terroristas, [chamo assim] porque isso não deixa de ser uma forma brutal de ser atacado e [incluo] os reflexos que causam à organização.

A empresa que nos atacou, em um ano, fez mais de 700 ataques no mundo. É um grupo terrorista de fora do Brasil que investiu contra diversas companhias, aqui e no mundo. Trabalho há muitos anos e, do ponto de vista profissional, foi a situação mais difícil que enfrentei na vida. Desligamos a companhia 100% por alguns dias.

Fomos fortemente impactados e impactamos também os nossos clientes. O processo foi duríssimo.

O resultado da empresa no ano passado, do ponto de vista de margem, teve um impacto de US$ 46 milhões. Isso praticamente destruiu o nosso resultado [de 2021]. Sofremos no primeiro trimestre deste ano e um pouco agora no segundo trimestre.

Fonte: Site Universo On Line (UOL) **Disponível em**: https://economia.uol.com.br/noticias/redacao/2022/08/15/entrevista-uol-lideres-dimitrius-oliveira-presidente-atento-america-do-sul.htm

IBRACON
Instituto de Auditoria Independente do Brasil

Potenciais impactos e implicações

Perda de Propriedade Intelectual

Incluindo materiais patenteados e de marca registrada, listas de clientes e dados sensíveis comerciais

Reputacional

Perdas que afetam o valor de mercado da empresa; perda da confiança dos consumidores e fornecedores.

Tempo

Aplicado na investigação dos incidentes e das perdas e para manter os investidores informados e atender as autoridades reguladoras

Penalidades, podendo ser multas por descumprimento legal ou regulatório

Devido a vazamento de dados ou compensações contratuais por atrasos e descumprimento de clausulas

Recursos administrativos

para corrigir os impactos como restaurar a confiança dos clientes, comunicações às autoridades, reposição de ativos e restauração da organização do negócio aos nível pré incidente.

IBRACON
Instituto de Auditoria Independente do Brasil

Modelo de Governança

IBRACON
Instituto de Auditoria Independente do Brasil

Alguns exemplos de ações dos reguladores

SEC – U.S. Securities and Exchange Comission

Release No. 33-11216, Cybersecurity Risk Mgmt, Strategy, Governance, and Incident Disclosure

A SEC divulgou suas regras finais sobre segurança cibernética, as quais abordam gerenciamento de riscos, estratégia, governança e divulgação de incidentes de segurança cibernética. Seu objetivo é fornecer informações mais consistentes, comparáveis e úteis para que os investidores possam avaliar melhor a exposição de uma empresa listada aos riscos e incidentes de segurança, e suas estratégias para mitigar esses riscos e incidentes.

Presidência da República

Lei 13.709 / 2018– Lei Geral de Proteção de Dados (LGPD)

Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Banco Central do Brasil

Res. CMN n° 4.893 de 26/2/2021 e Res. BCB n° 85 de 8/4/2021

Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições e instituições de pagamento, respectivamente, autorizadas a funcionar pelo Banco Central do Brasil.

Agência Nacional de Telecomunicações

Resolução nº 740, de 21/12/2020

Este Regulamento tem por objetivo estabelecer condutas e procedimentos para a promoção da segurança nas redes e serviços de telecomunicações, incluindo a Segurança Cibernética e a proteção das Infraestruturas Críticas de Telecomunicações.

Ato nº 2436, de 07/03//2023

Requisitos Mínimos de segurança cibernética para avaliação da conformidade de equipamentos CPE (*Customer Premises Equipment*)

Agência Nacional de Energia Elétrica

Res. Normativa Aneel 964 – 14/12/2021

Dispõe sobre a política de segurança cibernética a ser adotada pelos agentes do setor de energia elétrica (os concessionários, os permissionários e os autorizados de serviços ou instalações de energia elétrica; e as entidades responsáveis pela operação do sistema, pela comercialização de energia elétrica ou pela gestão de recursos provenientes de encargos setoriais.

Superintendência de Seguros Privados

Circular SUSEP Nº 638, de 27/07/2021

Dispõe sobre requisitos de segurança cibernética a serem observados pelas sociedades seguradoras, entidades abertas de previdência complementar (EAPCs), sociedades de capitalização e resseguradores locais.

IBRACON
Instituto de Auditoria Independente do Brasil

Cybersecurity Frameworks

ISO/IEC 27K Security Control Standards [1]

NIST Cybersecurity Framework [2]

ISF – Information Security Forum [3]

CIS – Center for Internet Security [4]

Disponível em:

[1] https://www.iso.org/home.html
[2] https://www.nist.gov/cyberframework
[3] https://www.securityforum.org/
[4] https://www.cisecurity.org/controls

IBRACON
Instituto de Auditoria Independente do Brasil

NIST Cybersecurity Framework v 1.1

Estrutura central do framework

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

IBRACON
Instituto de Auditoria Independente do Brasil

Responsabilidade da auditoria independente sobre Cybersecurity

21 de novembro de 2019 - Ano 10 - Nº 555

CRCSP ONLINE

INFORMATIVO SEMANAL

Opinião

Auditoria independente e a segurança cibernética

Francisco Sant'Anna*

A polêmica relativa à alegada invasão de mensagens de magistrados e promotores da Lava Jato no Telegram, aos até então apontado como invisível por seus criadores, expôs novamente os riscos inerentes à segurança cibernética e os cuidados a serem adotados para se evitarem danos às empresas, ao mercado financeiro e à economia. É inevitável encarar de frente o problema.

O tema merece atenção especial dos administradores de qualquer empresa, que, independentemente de seu ramo de atividade, cavizo ao alto nível de dependência tecnológica hoje existente, estão cada vez mais vulneráveis a ataques cibernéticos. Nessa linha, os profissionais de auditoria precisam estar cada vez mais preparados para auditar adequadamente a avaliação dos riscos de invasão nos sistemas de seus clientes.

A ação dos hackers pode ser muito nociva, em função do grau de informações que possam ser suprimidas e/ou alteradas e do nível de danos causados no sistema de informática da organização atacada. Há casos relatados em todo o mundo, há tempos, de saques e invasões de contas de correntistas de bancos, infiltração nos computadores de indústrias e organismos estatais.

Em 2018, por exemplo, segundo levantamento realizado pelo Gabinete de Segurança Institucional (GSI) da Presidência da República do Brasil, foram detectadas 20,6 mil notificações de incidentes computacionais em órgãos do governo, dos quais 9,9 mil foram confirmados, isso significa média de mais de um por hora. Desde 2014, o número de ataques não fica abaixo de nove mil.

Em abril de 2018, utilizando um pequeno computador do tamanho de um cartão de crédito, que custa 30 dólares, um hacker invadiu os sistemas do Laboratório de Propulsão a Jato da Nasa e acessou informações sigilosas. O problema foi relatado em junho de 2019. Investigações revelaram que o criminoso permaneceu dez meses atuando sem ser detectado e furtou

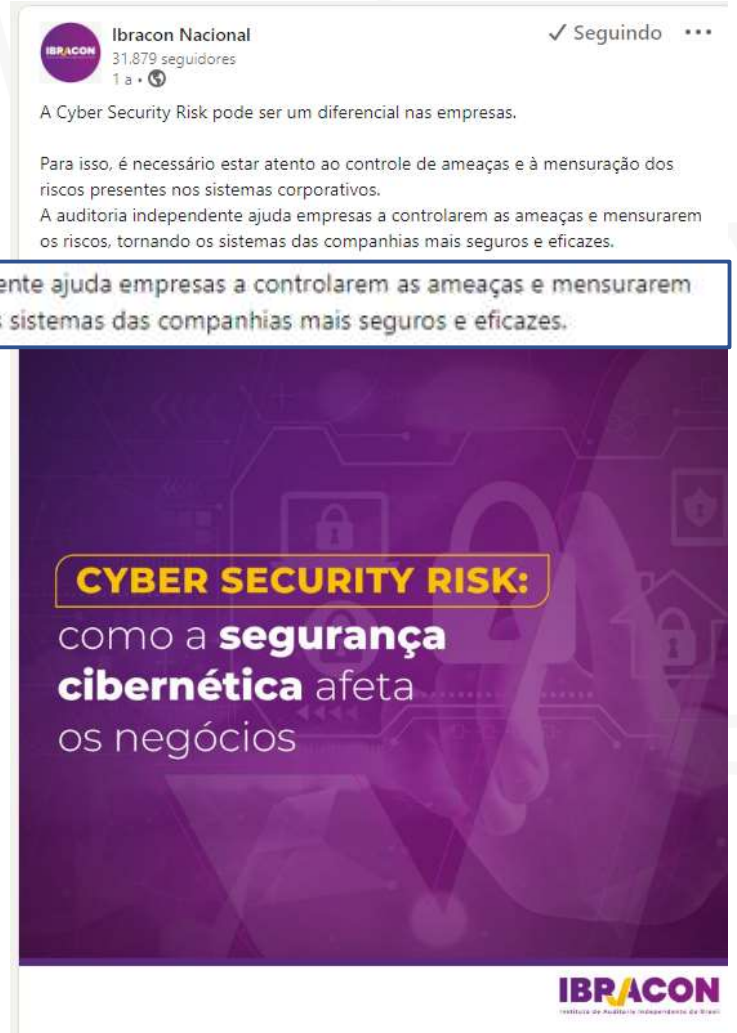
Nesse contexto de risco atual, os auditores independentes têm de se capacitar cada vez mais para fazer frente aos desafios presentes em seus serviços no tocante à segurança dos sistemas de tecnologia da informação das organizações auditadas.

Não é sem razão que as firmas associadas ao Ibracon - Instituto dos Auditores Independentes do Brasil investem, em média, 9% do faturamento em tecnologia, conforme revelou pesquisa da entidade. A categoria precisa estar cada vez mais preparada para atuar apropriadamente no campo minado dos ataques cibernéticos.

*Presidente do Instituto dos Auditores Independentes do Brasil (Ibracon).

voltar

Nesse contexto de risco atual, os auditores independentes têm de se capacitar cada vez mais para fazer frente aos desafios presentes em seus serviços no tocante à segurança dos sistemas de tecnologia da informação das organizações auditadas.



Fonte: CRCSP Online - **Disponível em**: https://crcsp.org.br/portal/publicacoes/crcsp-online/materias/555_07.htm

IBRACON
Instituto de Auditoria Independente do Brasil

OBRIGADO!

IBRACON

Instituto de Auditoria Independente do Brasil

Diretoria Nacional

www.ibracon.com.br

Acesse, curta e compartilhe: