Brasscom

Relatório de Cibersegurança 2025: Panorama e Insights

São Paulo, julho de 2025

Introdução

Este relatório tem como objetivo conscientizar sobre a importância da cibersegurança, reunindo em um único documento diversas informações estratégicas e relevantes sobre o tema. Ao oferecer um panorama detalhado do cenário atual da cibersegurança no Brasil, o relatório evidencia não apenas os desafios impostos pelos ataques cibernéticos, mas também a necessidade de investimentos estratégicos e estruturados para enfrentá-los de forma eficaz.

A crescente digitalização da economia amplia os riscos cibernéticos, mas também abre espaços para novas oportunidades. O aumento dos investimentos em cibersegurança representa uma oportunidade concreta para o setor de TIC, que pode se beneficiar com o desenvolvimento de novos negócios e ampliar a geração de receita por meio de soluções inovadoras e serviços especializados em segurança digital.

A Brasscom valoriza o trabalho contínuo de seus associados na promoção de práticas seguras e na implementação de medidas eficazes de proteção digital. Este relatório apresenta uma visão holística do estado da cibersegurança no Brasil, incluindo boas práticas, dados quantitativos e qualitativos, e reforça a importância de ações proativas nas organizações, como investimento, capacitação e estruturação estratégica, para garantir um ambiente digital seguro, resiliente e preparado para os desafios do futuro.

Resumo Executivo

R$104,6 Bi
Investimento Projetado
Entre 2025 e 2028 (+43,8%)

12º
Posição Global
No *market-share* de cibersegurança

16,1%
Crescimento anual
Profissionais de segurança da informação (2015–2024)

$1,36 Mi
Custo Médio
Violação de Dados no Brasil (2024)

60 Bi
Tentativas de Ataque
Em 2023

Phishing
Lidera como sendo o ataque mais comum

O Brasil se destaca globalmente em cibersegurança, mas investimentos estratégicos e estruturados são cada vez mais necessários

Postura reativa: Cibersegurança é reconhecida como prioridade, mas não se reflete proporcionalmente nos investimentos em processos estruturantes.

Segurança de TI é a **2ª iniciativa de TI** mais estratégica

Suporte executivo inadequado. Falta mais apoio para as medidas de segurança necessárias

3 PILARES DA CIBERSEGURANÇA: PESSOAS, PROCESSOS E TECNOLOGIAS

Trabalho Ético
Brasscom | ESG

Brasscom

Pessoas

As pessoas são essenciais e um dos pontos centrais da segurança cibernética pois o comportamento humano pode ser tanto uma linha de defesa quanto uma vulnerabilidade. Todos na organização, não apenas os profissionais de TI, devem agir de forma a ajudar a prevenir ataques e ajudar na proteção dos dados e sistemas.

Processos

Os processos englobam as políticas, normas e fluxos de trabalho que garantem a conformidade com padrões de segurança e minimizam os riscos da organização sofrer ataques. Além de lidar com ameaças, os processos indicam como gerenciar crises e monitorar o acesso a informações críticas.

Tecnologias

A tecnologia é um pilar essencial na cibersegurança, ampliando a capacidade de prevenção e defesa e fornecendo ferramentas como firewalls, criptografia e sistemas de detecção de intrusão para proteger redes e dados. Além de bloquear ameaças, possibilita a automação, respostas rápidas a incidentes e o monitoramento contínuo.

Cibersegurança no Brasil

Os dados mostram um cenário promissor, mas que ainda exige evolução na maturidade interna das organizações

- O Brasil é reconhecido como referência global em cibersegurança, com nota máxima em medidas legais, técnicas e de cooperação internacional.
- Apesar disso, ainda há espaço para avanços em estrutura organizacional, capacitação e conscientização, visto que também é um dos maiores alvos de ataque cibernético.
- O país ocupa a 12ª posição no mercado global de segurança cibernética e projeta investir R$104,6 bilhões entre 2025 e 2028.

Cibersegurança no Brasil

Trabalho Ético
Brasscom | ESG
Brasscom

Aumento de ataques digitais e violações de dados a cada ano

Brasil é um dos principais alvos de ataques cibernéticos do mundo

Escassez de mão de obra qualificada aumenta gastos e dificulta a proteção dos sistemas

Brasil investe em iniciativas para suprir lacuna de profissionais, como o programa Hackers do Bem

Fonte: Brasscom

Definição de Cibersegurança

Cibersegurança, ou segurança cibernética, é a prática de proteger sistemas, redes, dispositivos, aplicativos e dados de ameaças cibernéticas. É um ecossistema de proteção necessário para prevenir crimes cibernéticos e fraudes. O objetivo é evitar que os dados sejam acessados, destruídos, extorquidos ou que as operações de negócios sejam interrompidas.

Segundo o dicionário Oxford Online, segurança cibernética significa: O estado de proteção contra o uso criminoso ou não autorizado de dados eletrônicos, ou as medidas tomadas para conseguir isso.

Estrutura da Segurança Cibernética no Brasil

Trabalho Ético Brasscom | ESG

Brasscom

Gabinete de Segurança Institucional da Presidência da República GSI/PR

Responsável por coordenar a Política Nacional de Segurança da Informação (PNSI)

CGSI - Comitê Gestor da Segurança da informação

Assessora o GSI/PR nas atividades relacionadas à segurança da informação.

CNCiber – Comitê Nacional de Cibersegurança

Coordena as políticas e estratégias de segurança digital em âmbito nacional, atuando especialmente na gestão de crises e proteção de infraestruturas críticas. Ele colabora com diferentes setores para enfrentar ameaças cibernéticas e garantir a resiliência digital do país.

ComDCiber - Comando de Defesa Cibernética:

É o órgão do Exército Brasileiro que coordena a defesa cibernética do país, está ligado ao Ministério da Defesa

CGI.br - Comitê Gestor da Internet no Brasil:

Grupo de trabalho que define diretrizes para o uso e desenvolvimento da internet no Brasil, é multissetorial, com governo, comunidade cientifica e terceiro setor em sua composição

ANPD - Autoridade Nacional de Proteção de Dados:

Fiscaliza e regulamenta o cumprimento da Lei Geral de Proteção de Dados (LGPD). A ANPD também orienta e promove a cultura de proteção de dados pessoais. Ligada ao Ministério da Justiça e Segurança Pública

CISC gov.br - Centro Integrado de Segurança Cibernética do Governo Digital:

Atua na prevenção, tratamento e resposta a incidentes cibernéticos no gov.br, ligado ao Ministério da Gestão e Inovação em Serviços públicos

SRCC- Serviço de Repressão a Crimes Cibernéticos:

Investiga e combate crimes virtuais, como invasões de sistemas, roubo de identidade, e disseminação de malware, ligado à Polícia Federal

Subcomissão de Defesa Cibernética:

Parte da Comissão de Relações Exteriores e de Defesa Nacional no Senado, a Subcomissão de Defesa Cibernética propõe e avalia diretrizes estratégicas para a defesa digital no Brasil. Além de fiscalizar e acompanhar o trabalho do CNCiber, promove debates e audiências públicas para aprimorar as políticas de segurança cibernética

Banco Central do Brasil - Departamento de Tecnologia da Informação (Deinf):

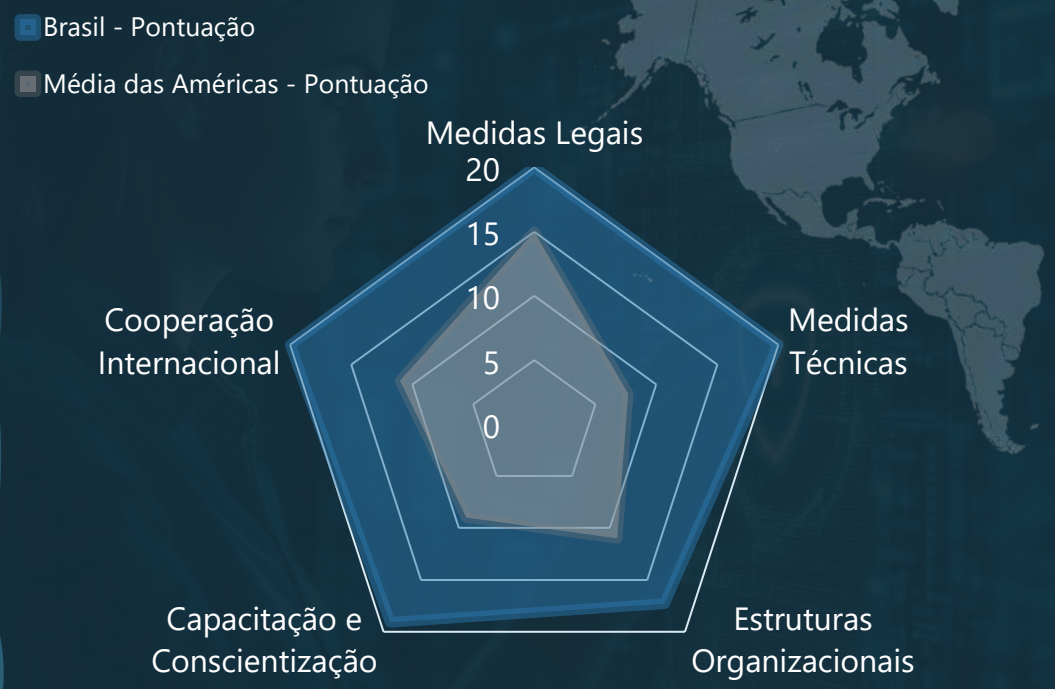
Coordena ações de cibersegurança, define políticas, realiza monitoramentos e atua na prevenção e resposta a incidentes. O Banco Central regula o setor financeiro em termos de cibersegurança com a Resolução CMN nº 4.893/2021. E também participa de fóruns e grupos como: GT-Ciber (Grupo de Trabalho de Cibersegurança da Febraban); GFIN (Global Financial Innovation Network); FSB (Financial Stability Board), incluindo a área de resiliência cibernética em sistemas financeiros globais.

Brasil é considerado país modelo em comprometimento com cibersegurança (Global Cybersecurity Index 2024)

O Brasil é o **único país da América do Sul com alta pontuação em maturidade de cibersegurança**, e um dos dois de toda a América que fazem parte do "Tier 1" na **nova forma de classificação** adotada pela 5ª edição do GCI, considerado assim um **país modelo no que tange ao comprometimento com a Agenda Global de Segurança Cibernética da UIT** (União Internacional da Telecomunicações). Entre os cinco pilares do GCI, o Brasil ainda tem oportunidades de avanço em dois: estruturas organizacionais e capacitação em cibersegurança. Isso envolve fortalecer a governança institucional e ampliar ações de formação, conscientização e desenvolvimento de competências digitais.

Em **2024**, a **UIT alterou sua metodologia**, passando de uma **classificação por posições individuais para uma categorização** em **grupos**, permitindo comparações mais claras entre países com características semelhantes. Essa **mudança visa destacar** como as **estratégias nacionais** impactam tanto o setor público quanto o privado, incentivando uma colaboração mais eficaz para impulsionar a transformação digital e promover um desenvolvimento equitativo no cenário global.

Performance em Ações Estratégicas para Cibersegurança (GCI)



Notas (Máximo 20):

Medidas Legais	Medidas Técnicas	Estruturas Organizacionais	Capacitação e Conscientização	Cooperação Internacional
20	20	17,3	19,1	20

Fonte: Brasscom, UIT - Índice Global de Segurança Cibernética 2024 (Global Cybersecurity Index – GCIv5)

TRAJETÓRIA GERAL DO BRASIL NO GLOBAL CYBERSECURITY INDEX (GCI) SUGERE ENGAJAMENTO E DESENVOLVIMENTO CONTÍNUO EM CIBERSEGURANÇA

Trabalho Ético Brasscom | ESG

Brasscom

EVOLUÇÃO DO BRASIL NO GLOBAL CYBERSECURITY INDEX (GCI):

- **GCI 2015**: Na 1ª edição (dados de 2013-2014), o Brasil obteve pontuação de **0,706**, alcançando a 5ª posição global.
- **GCI 2018**: Com nova metodologia baseada em rankings ponderados, o Brasil ficou em 6º nas Américas e 70º no ranking global, com **0,577** pontos.
- **GCI 2021**: O Brasil subiu para a 3ª posição nas Américas, com **96,60 pontos**. A metodologia foi revista, com redefinição das questões nos cinco pilares avaliados e a escala passou a ser de 0 a 100.
- **GCI 2024**: O país entrou no **Tier 1 – Role-modelling (pontuação entre 95 e 100)**, que reúne as nações com maior comprometimento com a cibersegurança. O modelo passou a adotar classificação por níveis de desempenho (tiers).

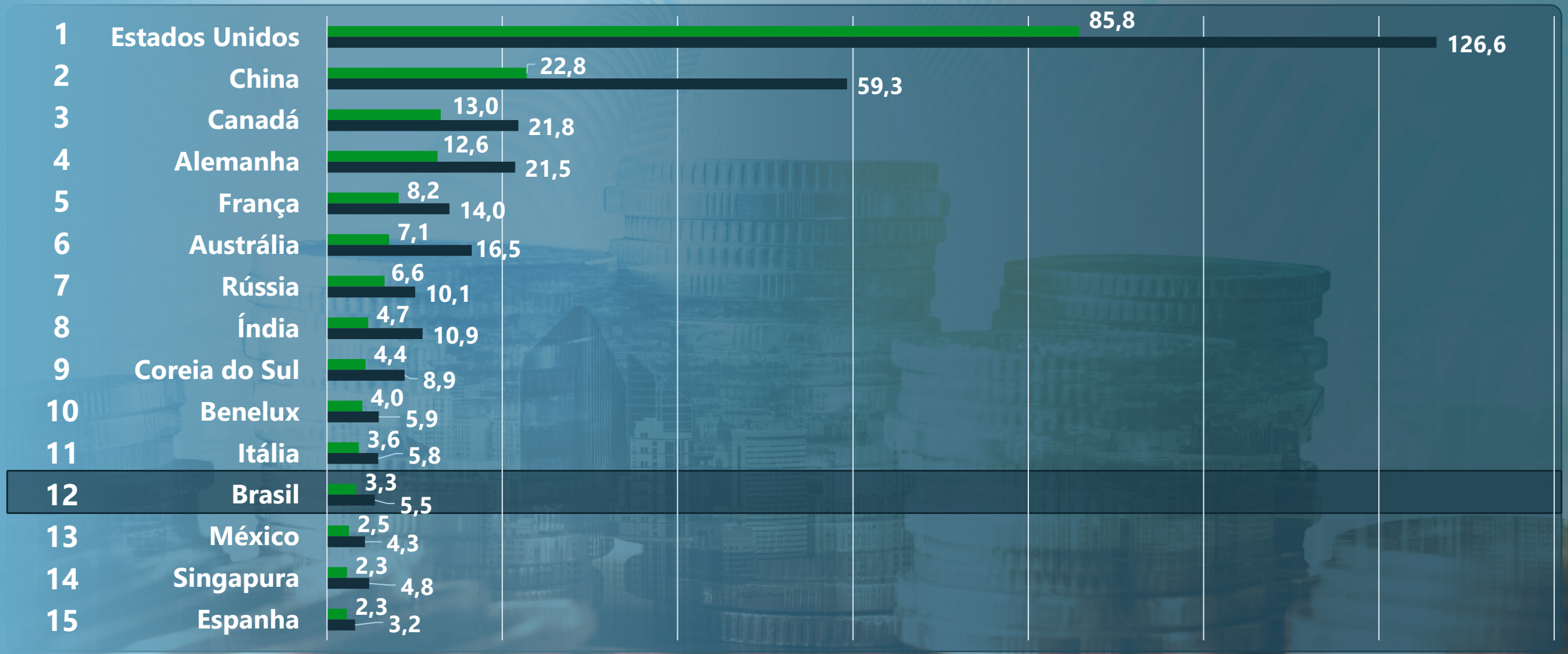
Fonte: Brasscom, UIT - Índice Global de Segurança Cibernética 2024, 2021, 2018, 2015 (Global Cybersecurity Index – GCI)

Brasil em 12° lugar no Mercado de Segurança Cibernética Global (2024)

O Tamanho do Mercado de Cibersegurança Global é US$ 207,8 Bi em 2024, com previsão de ser US$ 376,6 Bi em 2029

Trabalho Ético Brasscom | ESG

Brasscom



Fonte: Brasscom, Mordor Intelligence

Os investimentos globais estimados do usuário final com Segurança e Gerenciamento de Riscos em 2024 é de US$ 215 Bilhões (+14,3% que em 2023)

Em 2024, o governo Biden destinou **US$ 12,7 bilhões** para iniciativas de cibersegurança federal, o equivalente a um aumento de **13%** em relação ao ano anterior, com alocações principais voltadas para a Agência de Segurança Cibernética e Infraestrutura (CISA) e para a modernização de infraestrutura crítica.

Os gastos com segurança na Europa terão crescimento de **12,3%** em 2024. A previsão é de que o aumento de gastos seja contínuo entre 2022 e 2027, atingindo **US$ 84 bilhões** em 2027.

O governo do Reino Unido publicou em sua Estratégia Cibernética Nacional que iria investir **£ 2,6 bilhões** em 2022 para solidificar sua posição como uma potência cibernética global, além de financiamento adicional para a Força Cibernética Nacional

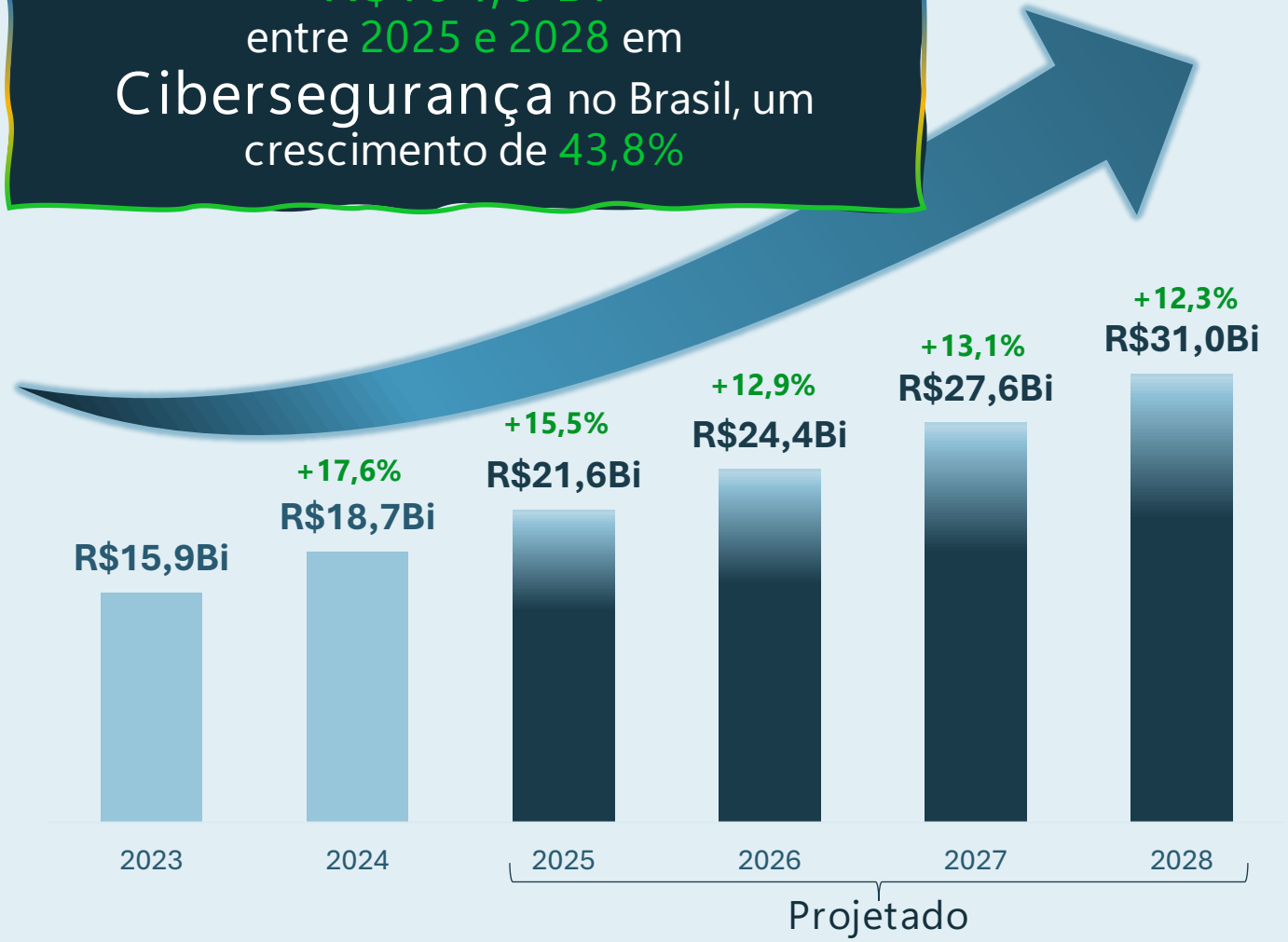
Fonte: Brasscom, MarketsAndMarkets (Cybersecurity-Industry-Outlook-2024), IDC (Worldwide Security Spending Guide), Reino Unido

Segurança da Informação é a 4ª tecnologia com maior projeção de gastos no Brasil para os próximos 3 anos

Trabalho Ético Brasscom | ESG

Brasscom

Projeção de Gastos de
R$104,6 Bi
entre 2025 e 2028 em
Cibersegurança no Brasil, um
crescimento de 43,8%



Fonte: Brasscom, IDC Black Book 3ª Plataforma, 2024V4.

Crescimento médio de 16,1% a.a. em empregos de Segurança da Informação
30 mil pessoas capacitadas na área pelo Hackers do Bem até o final de 2025

Trabalho Ético Brasscom | ESG

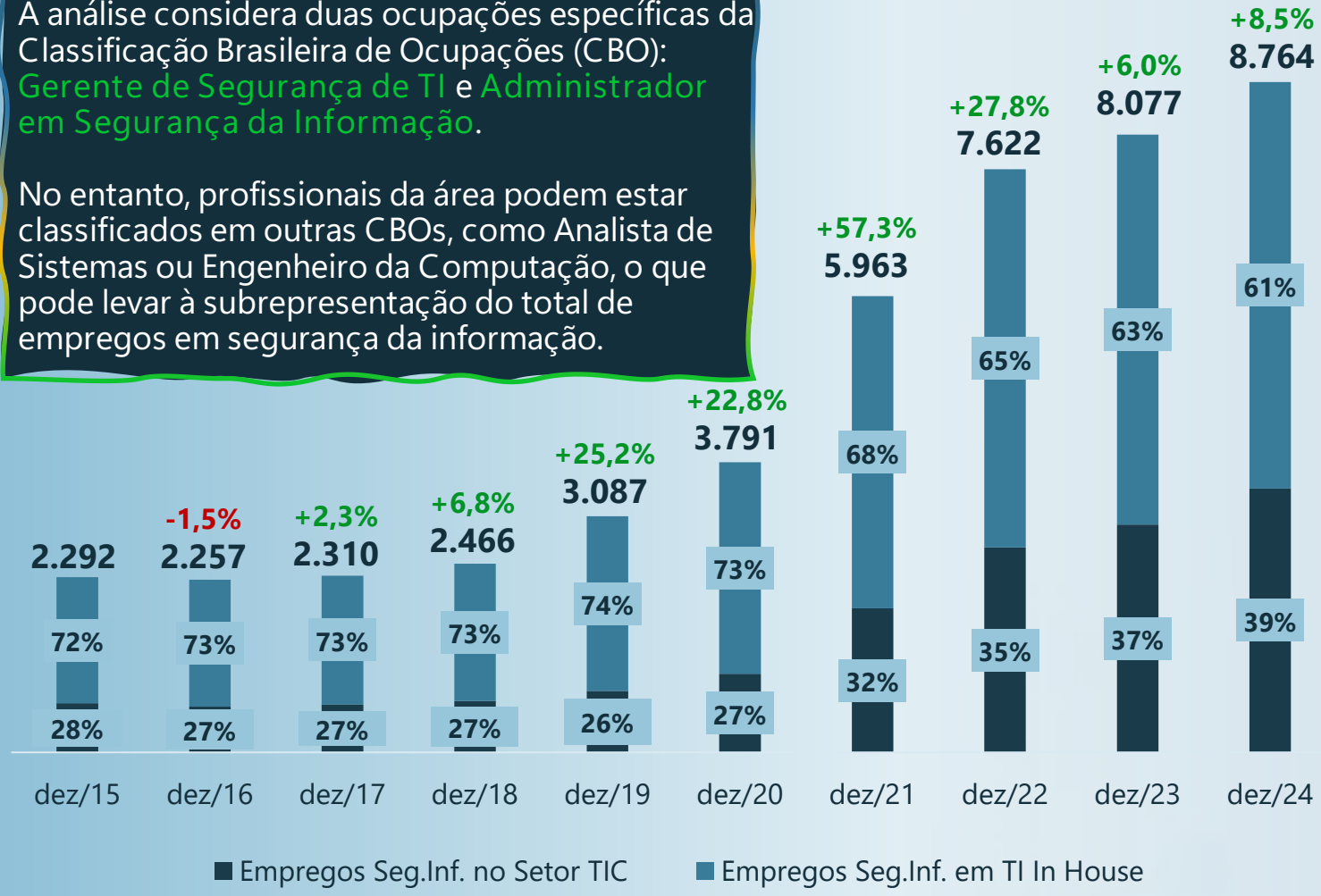
Brasscom

Empregados em Segurança da Informação no Brasil

% Crescimento de Empregos | Total de Empregos | % de Participação

A análise considera duas ocupações específicas da Classificação Brasileira de Ocupações (CBO): Gerente de Segurança de TI e Administrador em Segurança da Informação.

No entanto, profissionais da área podem estar classificados em outras CBOs, como Analista de Sistemas ou Engenheiro da Computação, o que pode levar à subrepresentação do total de empregos em segurança da informação.



O número de graduados em Segurança da Informação em 2023 foi de 1.849, um aumento de 15,3% em relação ao ano anterior, 2022

Com um investimento de R$ 32,6 milhões, o programa Hackers do Bem visa capacitar 30 mil profissionais em cibersegurança até o final de 2025. Desde seu lançamento, em 2023, mais de 120 mil pessoas já se inscreveram no projeto

São valorizadas competências como programação, conhecimento de redes e sistemas e de resolução de problemas, habilidades adquiridas através de cursos, treinamentos e certificações, sem exigir um diploma formal específico para atuar na área

Fonte: Brasscom, RAIS, CAGED, INEP (Censo da Educação Superior 2023),RNP (Hackers do Bem)

Ataques Cibernéticos

Embora a transformação digital avance rapidamente, a proteção cibernética ainda precisa acompanhar esse ritmo com investimentos mais estratégicos e estruturados.

- O Brasil vive um paradoxo em cibersegurança: enquanto lidera em inovação no sistema financeiro, com soluções como o PIX e um dos Open Bankings mais completos do mundo, também se torna um alvo cada vez mais exposto a ataques cibernéticos.
- Em março de 2025, 38% da população brasileira foi vítima de golpe bancário (ou tentativa de golpe).
- O país registrou um total de 60 bilhões de tentativas de ataques em 2023.
- O custo médio de uma violação de dados no Brasil foi de US$ 1,36 milhão em 2024.

Processo de um Ataque Cibernético na visão do hacker

Cyber Kill Chain (Cadeia de Ataque Cibernético)

Busca por vulnerabilidades

Verificação do melhor método de ataque e armamento

Comprometimento do sistema pelo armamento sem alarmar mecanismos de segurança

Exploração da vulnerabilidade e primeiro acesso ao sistema da vítima

Criação de uma conexão, um backdoor onde o invasor pode entrar e sair sem ser detectado

Controle dos ativos e poder de manipulação sobre a vítima

Agora com acesso, o invasor prossegue com o seu objetivo inicial

Fonte: Brasscom, Lockheed Martin

Definição de Ataque Cibernético

Os ataques cibernéticos são tentativas de criminosos, indivíduos ou organizações mal-intencionados de acessar ilegalmente a rede de computadores de TI de uma organização para roubar dados, propriedade intelectual ou dinheiro, interromper operações comerciais e cadeias de suprimentos ou causar danos a empresa de outras maneiras.

O principal ataque cibernético no Brasil, por incidência, é chamado de Phishing, onde o criminoso cria uma isca como um e-mail com urgência, induzindo a vítima a clicar em um link falso ou usar um site clonado que imita o original, obtendo assim dados sensíveis a partir de programas nocivos.

Rol de Principais Ataques Cibernéticos

Os dados de incidência dos ataques apresentados aqui foram retirados do relatório da Verizon sobre Investigações de Violação de Dados (DBIR) de 2025, que revela um panorama detalhado da **segurança cibernética global**, com base em mais de 22 mil incidentes e 12 mil violações confirmadas.

Ransomware	Malware que criptografa os dados da vítima, exigindo um resgate para a recuperação	Presente em 44% de todas as brechas.
Phishing	Táticas para enganar usuários e obter informações sensíveis (como senhas e dados bancários) através de e-mails ou mensagens fraudulentas.	Dos 4.009 incidentes mapeados, 85% resultou em violação dos dados.
Ataques DDoS	**(Distributed Denial of Service):** Sobrecarga de um sistema ou rede com tráfego excessivo, tornando-os inacessíveis.	6.520 incidentes, mas apenas 2 resultaram em violação de dados.
Exploração de Vulnerabilidades	Ataques que exploram falhas em software ou sistemas para ganhar acesso não autorizado.	Presente como vetor inicial em 20% das brechas.
Web Skimming	Inserção de código malicioso em sites de comércio eletrônico para roubar dados financeiros dos usuários durante transações.	Dos 1.701 incidentes, 82% resultaram em violação de dados.
Malware	Software malicioso projetado para danificar, desabilitar ou acessar sistemas sem autorização.	Dos 9.124 incidentes, 80% resultaram em violação de dados.

Fonte: Brasscom, Verizon (DBIR,2025)

Brasil: Sistema Bancário Moderno x Ataques

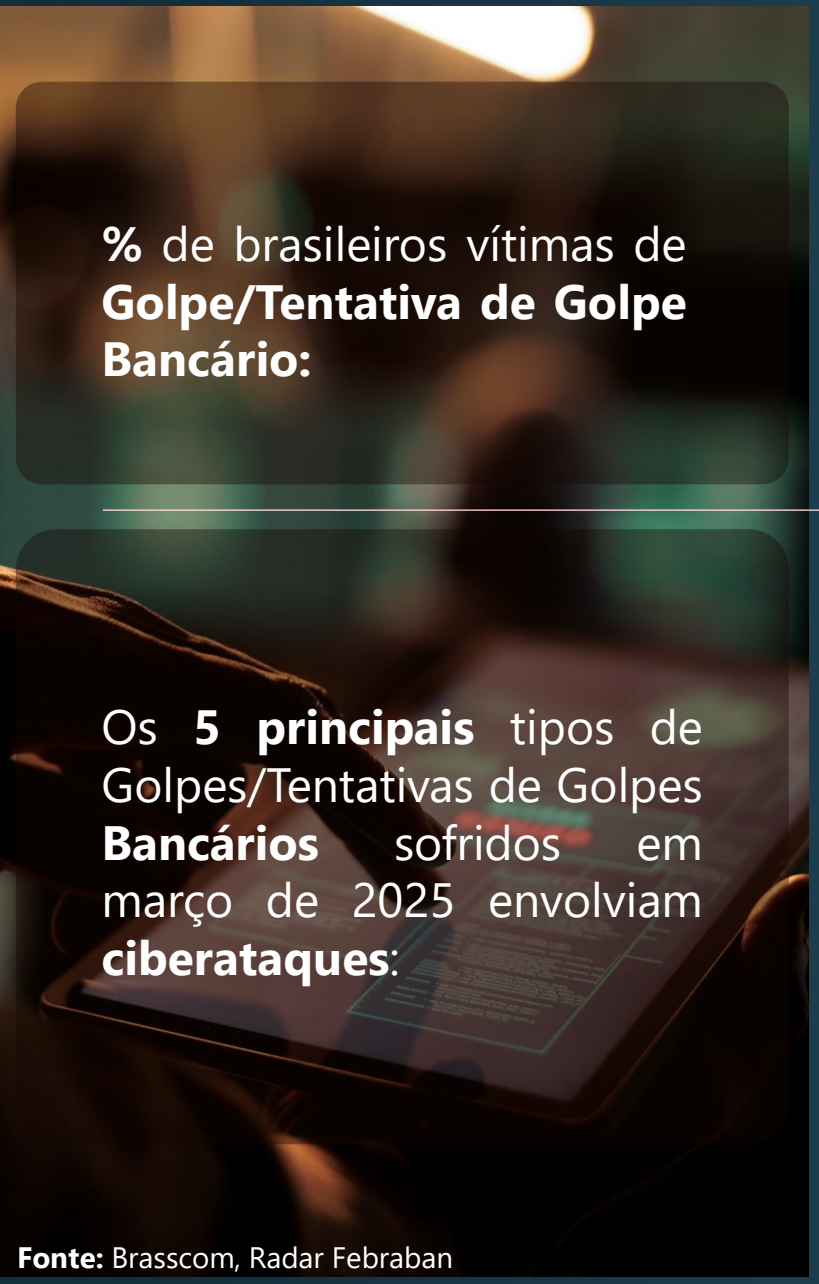
Trabalho Ético Brasscom | ESG

Brasscom

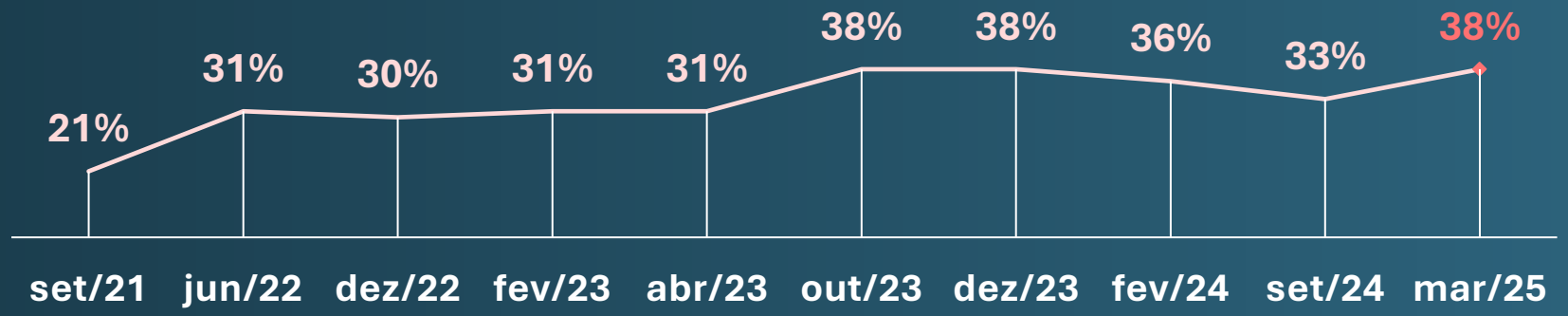
- O Brasil é considerado um dos países com os sistemas bancários mais avançados e modernos do mundo em termos de inovação e digitalização.
- São movimentados mensalmente **R$1,5 trilhão** pelo **PIX**, que foi implementado há 3 anos no Brasil.
- Em março de 2025, **38%** da população brasileira foi vítima de um golpe bancário ou tentativa de golpe, um aumento de **5 p.p.** em relação à setembro de 2024: **33%**.
- O Open Banking no Brasil é um dos mais completos do mundo, permitindo uma nova forma de interação entre consumidores e instituições financeiras ao ser possível o compartilhamento de dados, melhor controle de informações, maior autonomia e transparência.
- Com o aumento e destaque da transformação digital em larga escala do sistema financeiro brasileiro, cresceu também a notoriedade e exposição do país a ataques cibernéticos.

Fonte: Brasscom, Banco Central do Brasil, Apura, Radar Febraban

Principais Golpes Bancários



% de brasileiros vítimas de **Golpe/Tentativa de Golpe Bancário:**



Os **5 principais** tipos de Golpes/Tentativas de Golpes **Bancários** sofridos em março de 2025 envolviam **ciberataques**:

40% ❖ Golpe da clonagem de cartão de crédito ou troca de cartões
- Captura dos dados da tarja/chip do cartão via dispositivos físicos ou digitalização

28% ❖ Alguém se fazendo passar por um conhecido solicitando dinheiro por WhatsApp
- Uso de engenharia social em plataformas digitais para simular identidade e pedir dinheiro

26% ❖ Golpe da central falsa onde alguém pede seus dados por telefone
- Phishing por ligação telefônica passando-se por atendente oficial para roubar dados sensíveis

16% ❖ Golpe do Pix
- Varia conforme o vetor, podendo ser link malicioso, QR falso ou engenharia social com urgência

11% ❖ Golpe com utilização do CPF através de SMS
- Envio de mensagens SMS falsas com links maliciosos para captura de dados pessoais

Fonte: Brasscom, Radar Febraban

Brasil é um dos maiores alvos de ataques cibernéticos no mundo

Trabalho Ético Brasscom | ESG

Brasscom

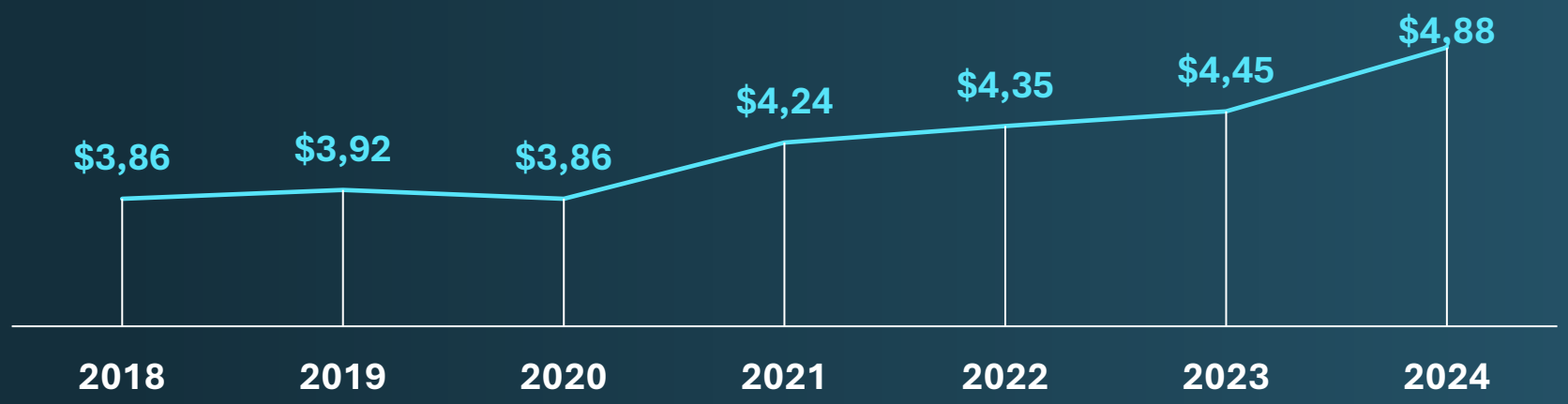
Brasil sofreu **60 bilhões de tentativas de ataques cibernéticos em 2023**, enquanto em 2022 registrou um total de **103 bilhões**

Em 2023, o montante de tentativas de ataques direcionados à América Latina foi de **200 bilhões**, 14,5% do total global nesse ano

93% dos líderes cibernéticos e **86%** dos líderes empresariais acreditam que a instabilidade geopolítica pode desencadear um **evento cibernético de grande escala** nos próximos dois anos. (WEF, 2024)

Fonte: Brasscom, FortiGuard Labs (Fortinet), WEF, NetScout

CUSTO MÉDIO TOTAL GLOBAL DE UMA VIOLAÇÃO DE DADOS (US$ MILHÕES)



CUSTO DE UMA VIOLAÇÃO DE DADOS POR PAÍS OU REGIÃO (US$ MILHÕES)

1º	2º	3º	4º	5º	• • •	16º
EUA 2024: $ 9,36 2023: $ 9,48	Oriente Medio 2024: $ 8,75 2023: $ 8,07	Benelux 2024: $ 5,9 2023: -	Alemanha 2024: $ 5,31 2023: $ 4,67	Itália 2024: $ 4,73 2023: $ 3,86		Brasil 2024: $ 1,36 2023: $ 1,22

Em 2024, o Brasil teve o **terceiro maior aumento** no custo de violação de dados (11,5%), atrás apenas da Itália (22,5%) e Alemanha (13,7%).

Fonte: Brasscom, IBM (2024)

Desafios da Cibersegurança no Ambiente Corporativo Brasileiro

Embora o Brasil esteja entre os primeiros a adotar novas tecnologias (early adopter), a implementação prática e a consolidação dessas soluções em estratégias robustas de segurança ainda são limitadas (late finisher).

- Postura pouco proativa das empresas brasileiras ainda travam o desenvolvimento da Cibersegurança no Brasil, apesar das perspectivas de expansão de investimento em segurança por parte das empresas.
- Mercado brasileiro segue sendo retratado com “early adopter, but late finisher”.
- O custo médio global de uma violação de dados foi de US$ 4,88 milhões em 2024.

Desafios do cenário de cibersegurança e violação de dados

Custo Médio de uma Violação de Dados em 2024 foi de US$ 4,9 Mi

O custo médio de uma violação de dados em 2024 foi de **US$ 4,88 milhões**, 10% a mais que em 2023 (IBM, 2024). Além disso, o uso extensivo de IA na prevenção de ataques refletiu uma economia média de **US$ 2,2 milhões**.

Suporte Executivo Inadequado

69% dos respondentes de uma pesquisa da Kyndryl (Cyber Gauge, 2024) relataram falta de apoio dos líderes empresariais para as medidas de segurança necessárias, e **73%** indicaram que há desinteresse no nível do conselho na prontidão de segurança, o que dificulta o enfrentamento às ameaças.

Escassez de Profissionais e Skills em Cibersegurança

Mais da metade das organizações violadas enfrentam altos níveis de escassez de pessoal de segurança (IBM, 2024). Essa questão representa um **aumento de 26,2%** em relação a 2023, uma situação que correspondeu a uma média de **US$ 1,76 milhões a mais** em custos de violação em 2024.

Fonte: Brasscom, IBM, Kyndryl

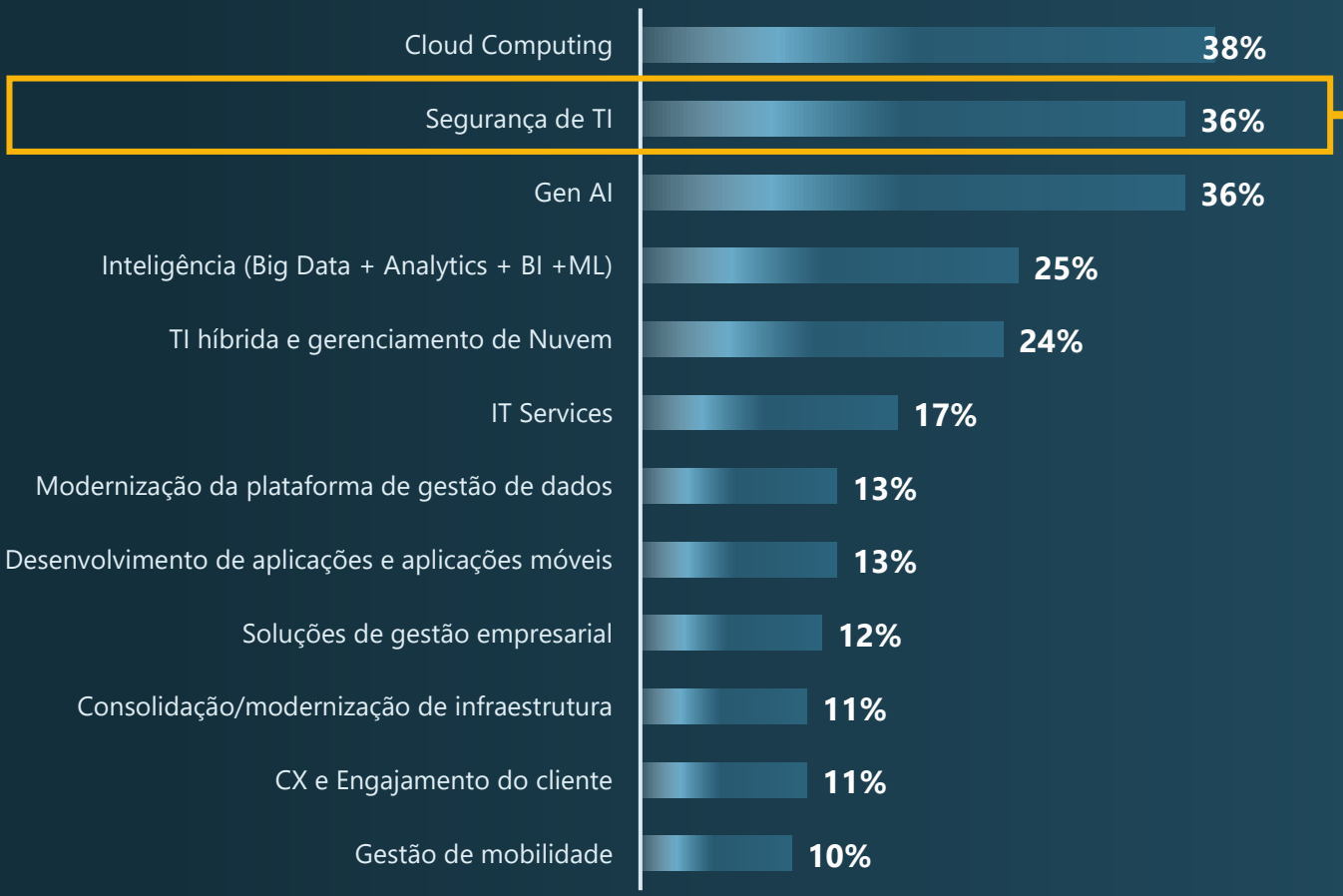
HÁ BASTANTE PREOCUPAÇÃO COM O TEMA POR PARTE DAS EMPRESAS MAS AINDA POUCO INVESTIMENTO

Trabalho Ético Brasscom | ESG

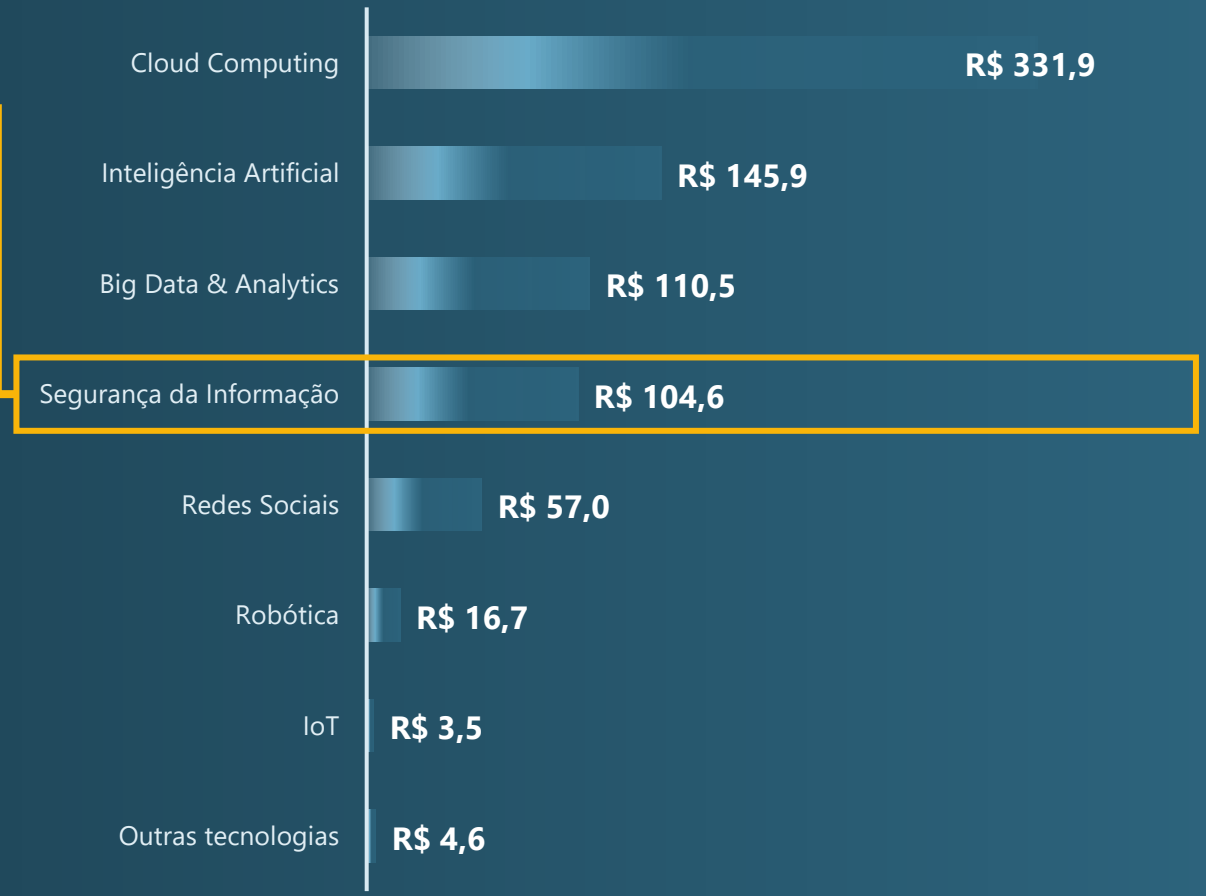
Brasscom

Embora a segurança de TI seja a **segunda maior prioridade** para as empresas em 2025, ela aparece apenas em **quarto** lugar nas intenções de investimento em tecnologias digitais, indicando uma possível lacuna entre a percepção de importância e a alocação efetiva de recursos.

Importância Estratégica das iniciativas de TI



Perspectivas de Investimentos em tecnologias digitais (R$ Bi) 2025-2028



Fonte: Brasscom, IDC (IT Investment Trends 2025 | n=100)

Desafios enfrentados pelo CISO (Chief Information Security Officer) no ambiente corporativo

Trabalho Ético Brasscom | ESG

Brasscom

INFLUENCIADOR E NÃO DECISOR:

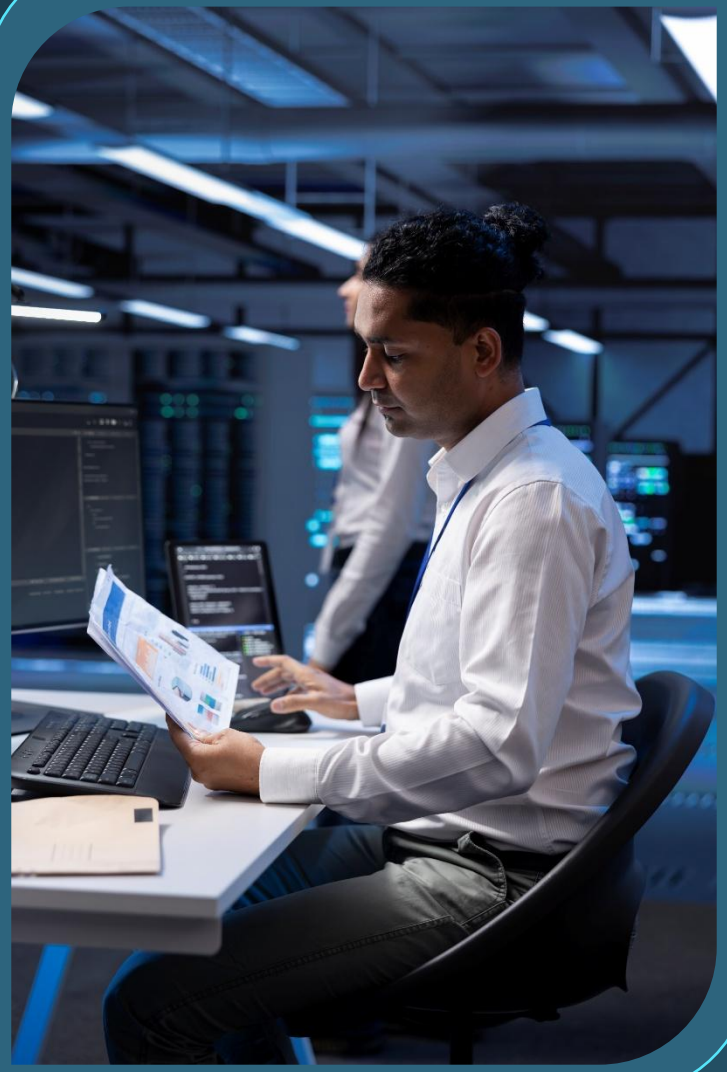
Embora reporte ao CIO, o CISO geralmente atua como influenciador e não como decisor direto sobre o orçamento. Frequentemente precisa negociar com o board para obter recursos, o que resulta em orçamentos fragmentados.

ATUAÇÃO TÁTICA:

Sua atuação tende a ser mais tática, voltada para o dia a dia operacional, o que dificulta o planejamento de longo prazo e a construção de uma visão integrada de segurança.

DIFICULDADE EM MENSURAR O VALOR DO RISCO CIBERNÉTICO:

Muitos tomadores de decisão não compreendem plenamente o que está em jogo. Embora segurança apareça como prioridade nas pesquisas de tendências tecnológicas, isso nem sempre se traduz em investimento real.



A falta de uma abordagem proativa, que antecipe riscos e integre segurança desde o design, ainda **impede avanços estratégicos e sustentáveis na maturidade de segurança das organizações.**

- Adoção de novas soluções costuma ser mais reativa do que planejada
- Ainda há a percepção equivocada de que cibersegurança é responsabilidade exclusiva da área de TI
- Essa visão leva a priorização de gastos com recuperação de incidentes em vez de investimentos em proteção ativa

Fonte: Brasscom, IDC (Brazil Breakfast Briefing, 2025)

COMPORTAMENTO "EARLY ADOPTER, BUT LATE FINISHER"

Trabalho Ético Brasscom | ESG

Brasscom

Embora o Brasil esteja entre os primeiros a adotar novas tecnologias (early adopter), a implementação prática e a consolidação dessas soluções em estratégias robustas de segurança ainda são limitadas (late finisher).

ALTA ADOÇÃO DE TECNOLOGIA, MAS BAIXA MATURIDADE EM SEGURANÇA

97% dos líderes brasileiros acreditam que tecnologias avançadas, como inteligência artificial, serão fundamentais na defesa contra ataques cibernéticos. No entanto, apenas **um terço** das empresas no Brasil já utiliza IA em suas operações de cibersegurança.

ALTA EXPOSIÇÃO A RISCOS, MAS BAIXA CAPACIDADE DE RESPOSTA ESTRUTURADA

79% das empresas brasileiras estão expostas a ataques cibernéticos. Mesmo reconhecendo os riscos, o problema está na dificuldade de transformar essa percepção em planos estruturados de proteção, o que evidencia um gap entre consciência e ação.

PRESSÃO SOBRE EQUIPES DE TI E FRAGMENTAÇÃO DE RESPONSABILIDADES

66% das equipes de TI no Brasil relatam sobrecarga devido ao aumento de incidentes de segurança. Embora as empresas estejam conectadas e tecnologicamente avançadas, a segurança ainda é tratada de forma reativa e fragmentada.

Fonte: Brasscom, The State of Cybersecurity in LATAM 2024, Grant Thornton (Riscos Cibernéticos — A percepção das lideranças brasileiras e práticas adotadas 2025)

Processo de Implementação de Segurança Cibernética

A segurança cibernética é um compromisso organizacional que exige investimento, planejamento e engajamento de todos os níveis da empresa.

Com apoio de políticas públicas, linhas de crédito e seguros especializados, mesmo pequenas e médias empresas podem estruturar defesas robustas contra ameaças digitais.

Implementação de Segurança Cibernética em uma organização

Etapas do Processo

Identificação e Avaliação Inicial

Identificar Ativos:
Listar ativos críticos (dados, sistemas, dispositivos).

Avaliar Riscos:
Determinar vulnerabilidades e potenciais ameaças.

Planejamento de Segurança

Definir Políticas e Normas:
Estabelecer diretrizes de segurança da informação.

Desenvolver Estrutura de Controles:
Planejar controles de segurança (tecnológicos, administrativos e físicos).

Implementação de Controles

Implantar Ferramentas de Segurança:
Firewalls, antivírus, sistemas de detecção de intrusão (IDS).

Aplicar Medidas Físicas:
Controle de acesso, vigilância e segurança de perímetro.

Configurar Permissões e Acessos:
Gerenciar permissões de acesso e autenticação dos usuários.

Treinamento e Conscientização

Educar Funcionários:
Realizar treinamentos sobre segurança cibernética.

Campanhas de Conscientização:
Implementar campanhas para aumentar a conscientização sobre ameaças, como phishing.

Monitoramento e Manutenção

Monitorar Atividades:
Implementar monitoramento de rede e logs de segurança.

Atualizar e Corrigir:
Realizar atualizações regulares de software e correções de vulnerabilidades.

Resposta a Incidentes

Estabelecer Procedimentos de Resposta:
Definir um plano de ação para responder a incidentes.

Identificar e Mitigar:
Detectar, conter e mitigar ameaças e ataques.

Revisão e Melhoria Contínua

Auditoria de Segurança:
Realizar auditorias periódicas para avaliar a eficácia das medidas implementadas.

Aprimorar Controles:
Ajustar políticas e controles com base em incidentes e novas ameaças.

Fonte: Brasscom

Investimento necessário para implementação de Cibersegurança varia de 200 mil a 41,8 milhões de dólares

Tamanho da Empresa	Orçamento Total de TI	Orçamento de Cibersegurança	% Cibersegurança vs Total de TI	Aumento planejado nos gastos de Cibersegurança*
Pequeno Porte funcionários < 500	US$ 1,6 Mi	US$ 0,2 Mi	12,5%	+8,8%
Médio Porte 500 < funcionários < 5000	US$ 10,5 Mi	US$ 1,2 Mi	11,6%	+9,2%
Grande Porte funcionários > 5000	US$ 41,8 Mi	US$ 5,7 Mi	13,6%	+8,5%

*** Aumento para 2025 e 2026**

Fonte: Brasscom, Kaspersky (IT Security Economics, 2024)

Recursos facilitadores para Implementação de Cibersegurança: Linhas de Financiamento e Seguros Cibernéticos

Linhas de Financiamento

São programas de crédito com taxas reduzidas para incentivar empresas a investirem em infraestrutura de cibersegurança, especialmente em pequenas e médias empresas.

Além de crédito acessível, algumas linhas oferecem consultoria para identificar as melhores soluções em cibersegurança, facilitando a escolha de tecnologias e práticas que se adequem ao risco específico de cada empresa. Uma das linhas de financiamento voltadas à implementação de soluções de cibersegurança é o BNDES, enquanto iniciativas voltadas à pesquisas, inovação e desenvolvimento contam com o apoio da FINEP. Já a Nova Indústria Brasil (NIB), embora não seja uma linha de financiamento, orienta políticas e instrumentos como BNDES e FINEP para promover a digitalização segura da indústria, tendo a cibersegurança como eixo estratégico da Missão 4.

Seguros Cibernéticos

São apólices que cobrem perdas financeiras e custos de recuperação após um ataque cibernético, ajudando na continuidade dos negócios e no gerenciamento de crises.

Com coberturas que variam conforme o setor e o perfil de risco, os seguros cibernéticos incluem opções de proteção contra ciberataques, vazamento de dados, responsabilidade por dados, extorsão cibernética e suporte para responder a falhas de conformidade, reduzindo impactos tanto financeiros como operacionais.

Fonte: Brasscom

INTERCONECTIVIDADE

Investir em cibersegurança é investir na continuidade e confiabilidade das operações digitais.

A interconectividade é um dos pilares da transformação digital, permitindo que dispositivos, sistemas e redes troquem dados em tempo real. No entanto, sem uma arquitetura de segurança bem definida, que combine tecnologia, processos e conscientização, ela se torna um vetor de risco.

INTERCONECTIVIDADE

A **interconectividade** permite que dispositivos e sistemas troquem dados, mas exige **segurança** para proteger informações e prevenir **ataques** e **fraudes**.

Plataforma de colaboração Online
Ferramentas de Drive precisam de segurança de dados para garantir confidencialidade.

Internet das Coisas (IoT)
Expansão de dispositivos conectados segurança reforçada para evitar ataques de dados.

5G e Leilão
A nova rede amplia conectividade, mas requer estratégias para mitigar vulnerabilidades e ataques avançados.

Governo Digital
Digitalização de serviços públicos demanda proteção contra acessos indevidos e fraudes.

Monitoramento Ambiental
Sensores conectados em áreas de monitoramento ambiental exigem segurança cibernética para evitar manipulação de dados.

Meios de Pagamento Digital
Sistemas de pagamento online exigem maior segurança para proteger informações financeiras.

Sistemas de Energia Inteligente
Redes de energia conectadas exigem mais segurança para prevenir ataques cibernéticos.

Escolas Conectadas
Expansão da internet no ensino exige medidas para proteger dados de estudantes e instituições.

Interconectividade e Segurança digital

Com a crescente digitalização, a **cibersegurança** deve ser integrada a todas as iniciativas de **interconectividade** para garantir a **proteção de sistemas, dados e usuários**.

Gerenciamento de Patches e atualizações
Processo de aplicar correções e atualizações de Software

Autenticação Multifatorial
Método de segurança com mais de uma verificação

Segurança em Nuvem
Proteção de dados armazenados em servidores remotos

Segmentação de rede
Divisão de rede em sub-redes

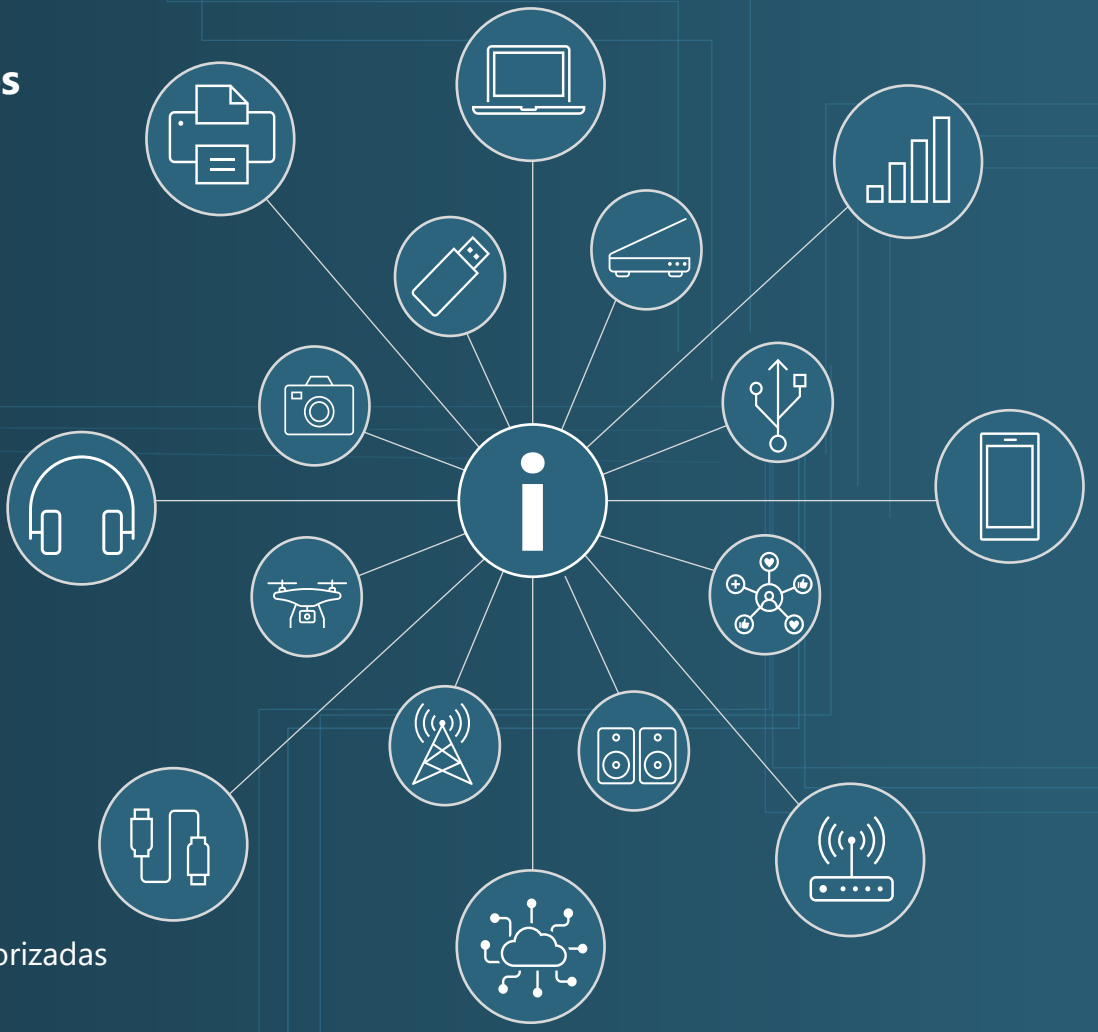
Firewalls
Sistema de segurança em monitoramento

Criptografia
Codificação de dados

Chaves Públicas
Criptografia com chave pública para descriptografar dados

Redes Privadas Virtuais (VPNs)
Tecnologia que conecta seguramente rede privada e pública

Monitoramento e detecção de intrusos
Técnica de vigilância de atividades suspeitas ou não autorizadas



Fonte: Brasscom, Brazilian-German Digital Dialogue - Quick guide on. VDMA, ABES

RECOMENDAÇÕES EM CIBERSEGURANÇA

Abordagem holística e adaptável, que integra pessoas conscientes e capacitadas, processos bem definidos e alinhados com as melhores práticas, e a utilização estratégica de tecnologias de segurança, com uma gestão de riscos contínua e colaboração entre diversos atores para fortalecer a resiliência no ambiente digital.

RECOMENDAÇÕES GERAIS EM CIBERSEGURANÇA

▶ PESSOAS

PROCESSOS

TECNOLOGIA

PRIORIZAR A CONSCIENTIZAÇÃO E O TREINAMENTO DOS USUÁRIOS

Muitas vulnerabilidades são causadas pelo mau uso dos usuários, tornando a informação, educação e treinamento essenciais para construir uma cultura de segurança.

MANTER-SE ATUALIZADO SOBRE AS DIVERSAS TÉCNICAS DE ATAQUES

A evolução dos ataques exige uma resposta contínua.

IMPLEMENTAR MEDIDAS BÁSICAS DE HIGIENE CIBERNÉTICA

Como a escolha de senhas fortes, a autenticação de dois fatores, a atualização regular de softwares e antivírus, e a realização de backups dos dados críticos. O acesso remoto a ambientes críticos deve requerer múltiplos fatores de autenticação.

Fonte: Brasscom (Contribuições da Brasscom à Consulta Pública sobre a Força-Tarefa contra Ransomware)

RECOMENDAÇÕES GERAIS EM CIBERSEGURANÇA

PESSOAS

▶ **PROCESSOS**

TECNOLOGIA

IMPLEMENTAR PROCESSOS DE SEGURANÇA BEM DEFINIDOS FÍSICOS E DIGITAIS
Estabelecer uma governança que organize a contínua identificação de riscos e as ações preventivas e corretivas necessárias.

PROMOVER A COLABORAÇÃO E O COMPARTILHAMENTO DE INFORMAÇÕES

Entre todas as partes interessadas, incluindo o setor privado, a academia e o governo

REALIZAR A GESTÃO DE RISCOS
Quantificar e gerenciar os riscos, estabelecendo meios para minimizar as vulnerabilidades e mitigar os danos

DESENVOLVER UMA CULTURA DE SEGURANÇA DA INFORMAÇÃO
A segurança da informação deveria ser um assunto cotidiano.

ESTAR ATENTO À SEGURANÇA DA INFORMAÇÃO COMO UM REQUISITO DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)
Estabelece diversos controles e responsabilidades para o tratamento de dados pessoais. Não há proteção de dados sem segurança da informação.

Fonte: Brasscom (Contribuições da Brasscom à Consulta Pública sobre a Força-Tarefa contra Ransomware)

RECOMENDAÇÕES GERAIS EM CIBERSEGURANÇA

PESSOAS

PROCESSOS

▶ TECNOLOGIA

UTILIZAR TECNOLOGIAS DIGITAIS PARA FORTALECER A SEGURANÇA DA INFORMAÇÃO

A nuvem democratiza o acesso à segurança, a IA aumenta a capacidade de responder dinamicamente a incidentes de segurança, uso de criptografia também é cada vez mais importante.

SEGURANÇA EM MÚLTIPLAS CAMADAS

Abrangendo computadores, redes, programas e dados. Uma postura de segurança bem-sucedida requer várias camadas de proteção.

Fonte: Brasscom (Contribuições da Brasscom à Consulta Pública sobre a Força-Tarefa contra Ransomware)

BOAS PRÁTICAS PARA INCIDENTES

Como reagir a um ataque Cibernético?

É importante lembrar que cada ataque cibernético é um incidente grave e único e requer conhecimento especializado para ser resolvido.

A depender da natureza do incidente, também são necessários avisos para as autoridades públicas responsáveis. Por isso, este relatório visa sensibilizar empresas e demonstrar possíveis pontos a serem considerados durante um incidente.

Primeira regra: em nenhuma circunstância efetue um login com todas as contas de administrador em um sistema potencialmente infectado, enquanto o sistema ainda estiver conectado à sua rede produtiva interna ou à Internet.

Isole os sistemas potencialmente infectados da rede imediatamente para evitar a disseminação do malware por meio de movimento lateral. Para fazer isso, desconecte o cabo de rede. Não desligue o dispositivo. Se necessário, crie um backup forense, incluindo uma imagem de memória para análises posteriores.

Gerenciamento de incidentes como um projeto

Fase 1 : Análise

- Identificação dos sistemas afetados;
- Prevenção de novas infecções e criptografia;
- Avaliação de danos;
- Análise do malware.

Fase 2 : Operação de transição

- Prevenção de novas infecções e criptografia;
- Bloqueio do acesso dos criminosos;
- Monitoramento intensivo da rede.

Fase 3 : Limpeza

- Concepção / implementação / reinicialização.

Fonte: Brasscom - Cartilha de Cibersegurança – International Digital Dialogues

Declaração de Uso

O conteúdo é de uso restrito da Brasscom e suas Associadas. A Brasscom não se responsabiliza por quaisquer usos que venham a ser feitos por terceiros, nem suas possíveis consequências nas esferas patrimonial, pessoal ou outras de qualquer natureza.

Liderança

Affonso Nina
Presidente Executivo

Mariana Oliveira
Diretora de Operações

Sergio Sgobbi
Diretor de Rel. Institucionais e Governamentais

Coordenação

Helena Loiola Persona
Coordenadora de Inteligência

Equipe

Ricardo Parrilla Novais
Analista de Inteligência

Mateus Ortega Mendes
Analista de Inteligência

Luana Lucio de Jesus
Assistente de Inteligência

Obrigado!

brasscom.org.br

Siga-nos nas redes sociais