Brasscom

RNP
REDE NACIONAL DE ENSINO E PESQUISA

Transformação digital acelerada e aumento dos riscos de ataques cibernéticos: como preparar a força de trabalho para estes desafios?

Sergio Paulo Gallindo

Presidente Executivo da Brasscom

Brasília 24 de maio de 2022

Associadas (87 Grupos Empresariais)

Brasscom

Fundadoras (08)

accenture · BRQ · Capgemini · IBM · Microsoft · TIVIT · TOTVS · UNISYS | Securing Your Tomorrow®

Plenas (04)

amazon · Embratel · HUAWEI · SONDA

Efetivas (43)

ADP · airbnb · Algar Tech · Apple · Atos · Bentley Advancing Infrastructure · ByteDance · Cast group · C.E.S.A.R · CI&T · CISCO · ClearSale · Cognizant · cpqd · DXC.technology · EQUINIX · facebook · FIS · GFT · hotmart · indra · Infosys · INGRAM MICRO · intuit · KUAISHOU · kyndryl · Linx · locaweb · LOGICALIS Business and technology working as one · NTT · OPTUM · ORACLE · salesforce · Senior Tecnologia para Gestão · serasa experian · spread · stefanini · tcs | TATA CONSULTANCY SERVICES · Telefónica · TIM · Uber · wipro · zoom

Colaboradoras (32)

a5 SOLUTIONS · Acesso Digital agora é UNICO · AMT SOLUTION DESK · apdata · assesso · AZION · BETHA · CERVELLO · Contmatic Phoenix · docwise gestão do conhecimento · δοxa DOXA ADVISERS · e-core · eSales · Ewave do Brasil · htp SOLUTION · impulso · idwall · ilia · INTELLIGENZA. IT & Business Solutions · keeggo · mandic CLOUD SOLUTIONS ESPECIALISTAS EM CLOUDS. · MERCADO BITCOIN · microblau CONTROLES E AUTOMAÇÃO · Neoway · ODATA · Plusoft · Prophix · Semantix · shipay · singia · SOLUTIS · SQUADRA Tecnologia

Modelos de Negócios

Serviços de TIC **(62)**

Software **(47)**

Big Data **(25)**

Segurança da Informação **(24)**

Nuvem ou Datacenter **(21)**

Inteligência Artificial **(20)**

Rede Social ou Plataforma **(15)**

Hardware **(10)**

Saúde Conectada **(8)**

Telecom **(7)**

Internet das Coisas **(5)**

Comércio Eletrônico **(4)**

Agricultura Digital **(4)**

Criptoativos **(1)**

Brasscom

Origem do Capital

(Quantidade de empresas)

América Latina

53% (46)

52% (45)

América do Norte

29% (25)

28% (24)

10% Europa (9)

8% Ásia (7)

Assembleia Geral

Órgão soberano, constituído pelo rol de associadas que, a cada dois anos, elegem o Conselho de Administração e Conselho Fiscal.

Conselho de Administração

Laércio Cosentino | TOTVS
Presidente do Conselho

Vice-Presidentes

Benjamim Quadros
BRQ

José Formoso
Embratel

Luiz Mattar
TIVIT

Maurício Cataneo
UNISYS | Securing Your Tomorrow™

Conselheiras (os)

Tânia Cosentino
Microsoft

Cleber Morais
amazon

Leonardo Framil
accenture
High performance. Delivered.

Marcelo Braga
IBM

Maurizio Mondani
Capgemini

Ricardo Scheffer
SONDA

Sun Baocheng
HUAWEI

Brasscom

Presidentes dos Órgãos Estatutários

Conselho Fiscal

Paulo Freitas
TIVIT

Comitê de Gentes

Laércio Cosentino
TOTVS

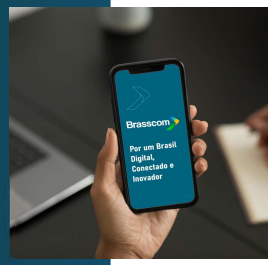
Comitê de Ética e Conformidade

Paulo Marcelo
SOLUTIS

Comitê de Relações Externas, Atração e Retenção

Elias Abdala
Microsoft

Por um Brasil Digital, Conectado e Inovador



Vida e Cidadania na Era Digital

Proteção de Dados Pessoais, Segurança da Informação, Inteligência Artificial, 5G, Internet das Coisas, Telemedicina e Agricultura Digital são fenômenos cada vez mais preponderantes em nossas vidas. Ao mesmo tempo, despertam para a necessidade de uma atuação voltada à garantia da segurança jurídica e à otimização das oportunidades que a era digital traz para as empresas e a própria sociedade.

Tributação, Emprego e Competitividade

A retomada da economia depende de reformas estruturantes que estimulem a competitividade e a geração de empregos no Brasil. Políticas públicas voltadas à racionalização do sistema tributário são essenciais para o país – contemplando a eficiência do Estado, por meio de um governo digital, e a redução da tributação sobre o trabalho, energia e Telecom.

Formação de Talentos em Tecnologia

A vocação dos brasileiros para a tecnologia e o crescimento exponencial do setor do TIC e de Tecnologias Digitais representam imensas oportunidades para o país. No entanto, para aproveitá-las, é necessário o enfrentamento da insuficiência de profissionais qualificados. Os desafios são: despertar, em jovens e adultos, o interesse por tecnologia; prover formação técnica e capacitação socioemocional; cuidar de um ambiente de diversidade nas instituições de ensino e empresas.

Brasscom Conexão Academia

Formação de Talentos

Ciência, Tecnologia e Inovação

41 Associadas Institucionais

Instituições de Ensino

Institutos de Pesquisa e Desenvolvimento

Conteúdo

O Macrossetor de TIC

Produção e crescimento do Macrossetor de TIC em 2021

(R$ bilhões)

	Macrossetor de TIC	TIC	TI In House	Telecom
Produção Setorial (R$/US$)	R$ 597,8 US$ 110,8	R$ 293,0 US$ 54,3	R$ 53,0[2] US$ 9,8	R$ 251,7 US$ 46,6
Proporção do PIB	6,9%	3,4%	0,6%	2,9%
Crescimento nominal (2020-2021)	+ 18,3% (+16,2 p.p.)	+ 36,4%[1] (+31,9 p.p.)	+ 6,4% (+1,8 p.p.)	+ 4,7% (5,0 p.p.)
Empregos (saldo 2021)	1,90 milhão + 198 mil	1,09 milhão + 129 mil	473 mil + 21 mil	330 mil + 21 mil
	TIC, TI In House e Telecom	TIC, Tecnologia da Informação e Comunicação: Software, Serviços, Nuvem, BPO, Estatais, Hardware e Exportações	Tecnologias Digitais nas empresas com outros objetos sociais	Voz, Celular e Dados Telecom e Serviços de Implantação

Cotação R$/US$ 5,40 (2021)
Var. cambial +4,7% (2020-2021)
Var. cambial +30,71% (2019-2020)

Notas:

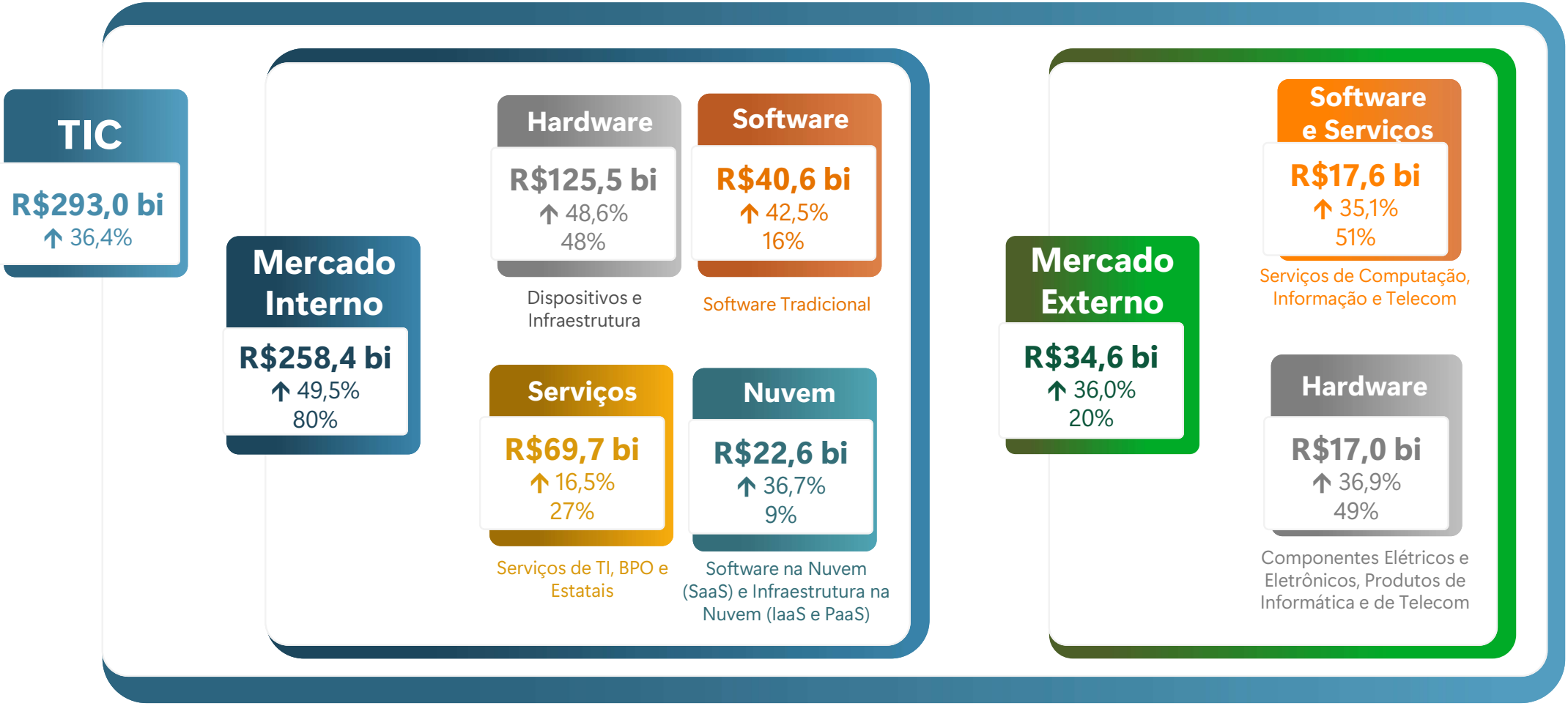
[1] O crescimento do setor de TIC está ligado à variação composta dos anos de pandemia

[2] Houve uma mudança metodológica do cálculo dos empregos pelas mudanças da estrutura dos dados do Novo Caged disponível nesse link, essa mudança impactou o cálculo da produção do TI In House que em termos de empregos novos o valor foi maior que o esperado.

FONTES: Brasscom, ABINEE, Bacen, IDC, Conexis Brasil Digital, Relatórios Financeiros das Estatais, RAIS e Caged.

Produção, crescimento e participação dos Subsetores TIC em 2021

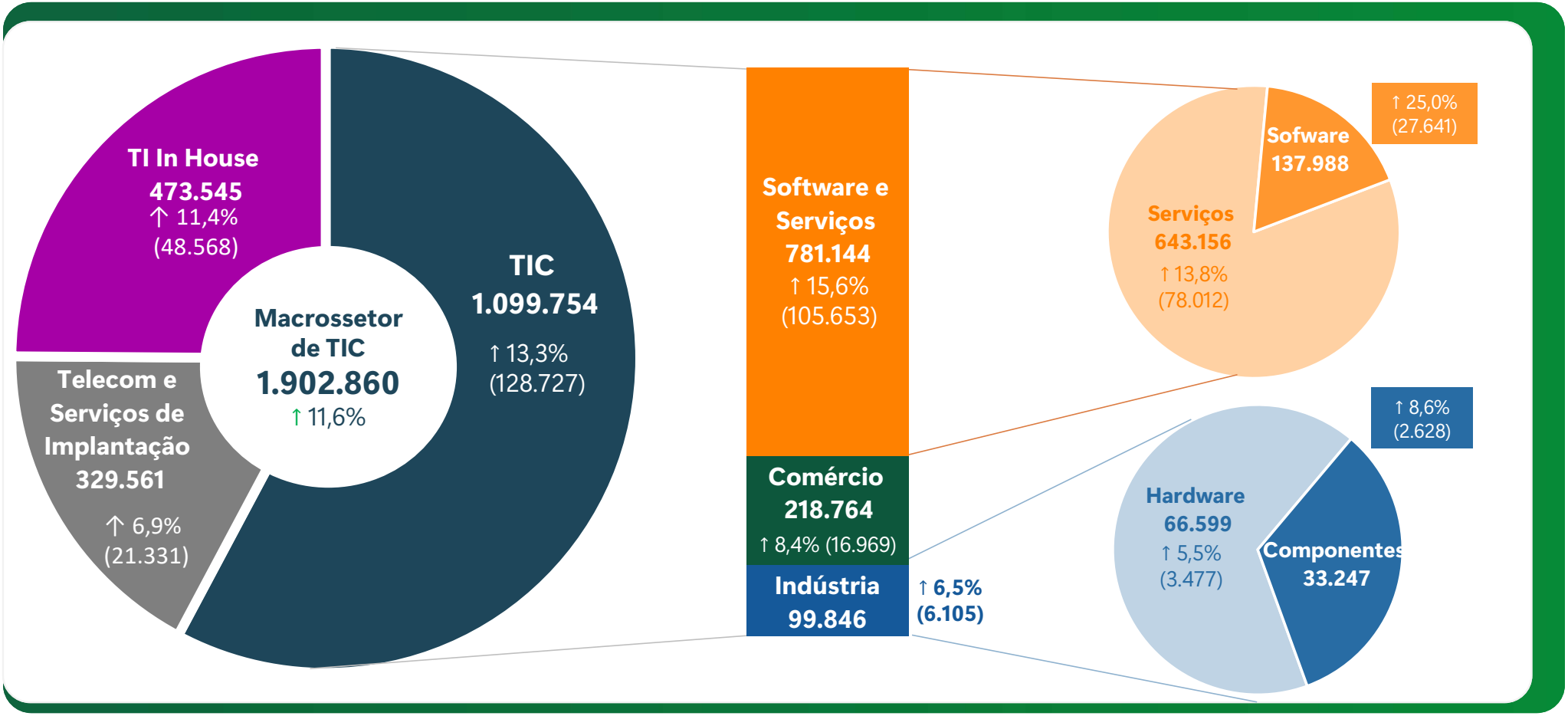
(R$ bilhões)



Nota: a metodologia da cálculo para a estimação da produção de BPO (*Business Process Outsourcing*) passou a considerar os valores publicados no Black Book do IDC.

FONTES: Brasscom, ABINEE, Bacen, IDC, Conexis Brasil Digital, Relatórios Financeiros das Estatais, RAIS e Caged.

Número de profissionais no Macrossetor de TIC em 2021



Notas:

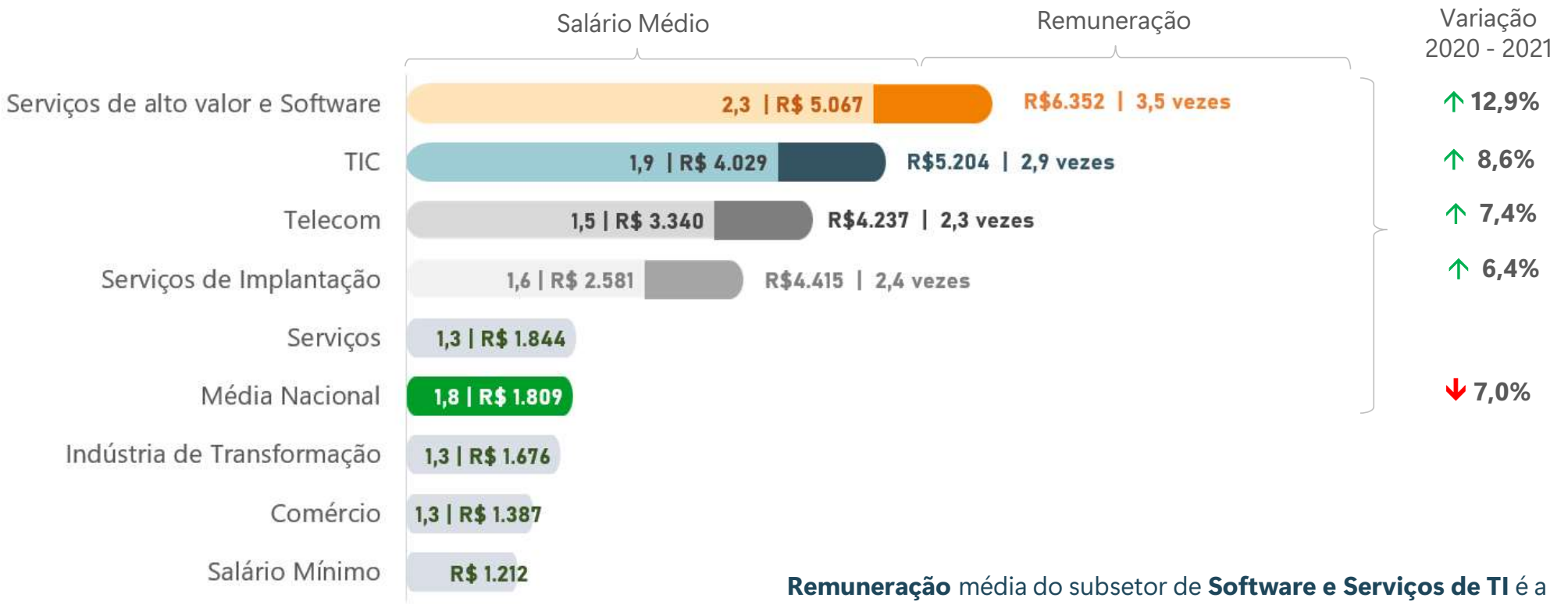
[1]Os empregos de nuvem estão dispersos em Software e Serviços.

[2]Serviços de implantação referem-se à prestação de serviços de planta externa, fibra ótica e instalação de cabos coaxiais. A partir da versão 2020 do Relatório Setorial, passamos a considerar os CNAEs (i) Construção de Estações e Redes de Telecomunicações e (ii) Manutenção de Estações e Redes de Telecomunicações.

FONTES: Brasscom, RAIS e Caged.

Salários de TIC e de Telecom no Brasil em 2021

Comparação da remuneração média de TIC e Telecom com salários médios setoriais e Nacional



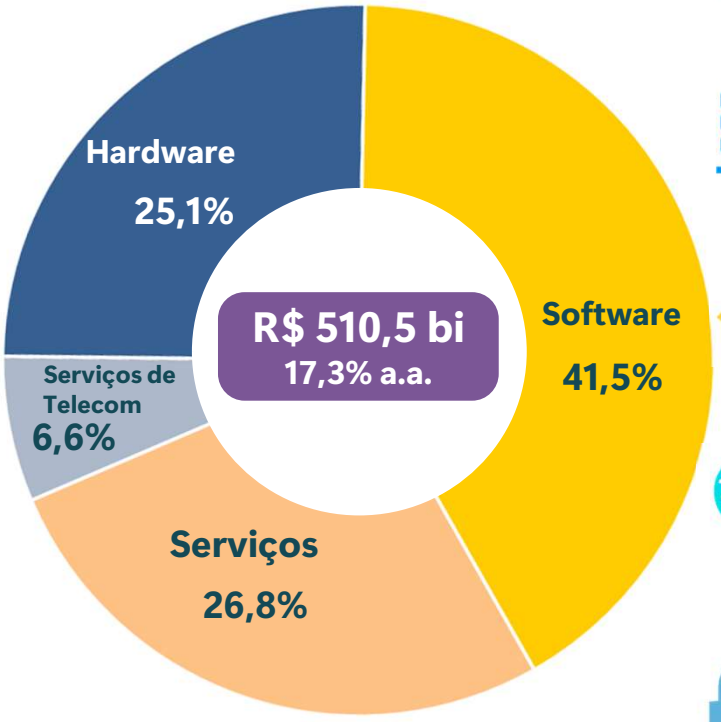
Remuneração média do subsetor de **Software e Serviços de TI** é a **maior** dentre as **pesquisadas,** e **3,5 vezes superior** ao **salário médio nacional.**

Nota metodológica: A remuneração do setor TIC, do subsetor de Serviços de alto valor agregado + Software e Telecom + Serviços de Implantação inclui benefícios comumente oferecidos no setor.
Obs.: Serviços de implantação referem-se à prestação de serviços de planta externa, fibra ótica e instalação de cabos coaxiais e Telecom refere-se às empresas de prestação de serviços de telecomunicações e infraestrutura de telecomunicações (por fio, por micro-ondas e por satélite).

Fonte: Brasscom, IBGE, RAIS e CAGED

Perspectivas de Investimentos de 2022–2025 (R$ bilhões)

Tecnologias de Transformação Digital



Nuvem
R$ 181,8 bi | 24% a.a.

Robótica
R$ 36,5 bi | 0,4% a.a.

Big Data & Analytics
R$ 94,6 bi | 12% a.a.

Redes Sociais
R$ 38,7 bi | 15% a.a.

Internet das Coisas
R$ 56,9 bi | 27% a.a.

Realidade Virtual
R$ 3,2 bi | 6% a.a.

Inteligência Artificial
R$ 49,7 bi | 18% a.a.

Blockchain
R$ 1,6 bi | 36% a.a.

Segurança da Informação
R$ 46,7 bi | 10% a.a.

Impressão 3D
R$ 0,8 bi | 14% a.a.

Mobilidade e Conectividade

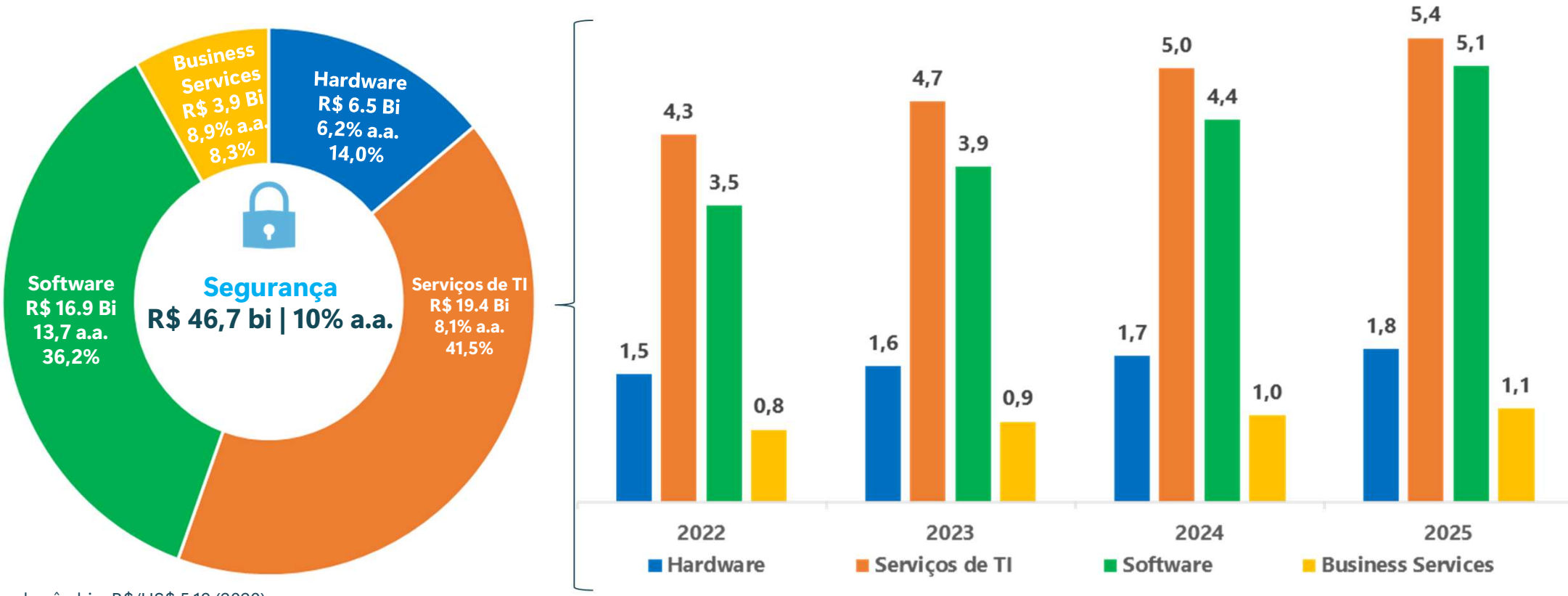
Mobile, Dados e Banda Larga

R$ 616,9 bi
9,3% a.a.

Fontes: Brasscom, IDC (Black Book Q4 2021, Black Book 3ª Plataforma, 2021 H1)

Taxa de câmbio: R$/US$ 5,40 (2021)

Perspectivas de Investimentos de 2022–2025 (R$ bilhões)



Taxa de câmbio: R$/US$ 5,19 (2020)

Nota: Business Services é atividades de consultoria e terceirização de processos. As demais categorias, Hardware, Software e Serviços de TI são considerados IT Services, ou seja, projetos orientados, terceirização, suporte e treinamento

Fontes: Brasscom, IDC (Black Book 3ª Plataforma, 2021 V4)

A Relevância da Segurança da Informação e da Segurança Cibernética

A escalada dos ataques e dos prejuízos das ações criminosas ao explorar novas vulnerabilidades em ambientes digitais solapam a confiança necessária para tornar a sociedade cada vez mais conectada e digital.

O Brasil e vários outros países sofreram os importantes ataques cibernéticos nos últimos dois anos e a previsão é que 2022 seja marcado pela continuidade dos ataques, especialmente de ransomware.

Ressalta-se, portanto, a importância da priorização da **Segurança da Informação e da Segurança Cibernética**, no âmbito governamental e privado, como caminho para garantir a **higidez das infraestruturas e dos serviços e a confiança no avanço da Era Digital.**

Principais ataques em 2021 – Brasil e Mundo

Jan
- TRF-3 foi alvo de ataque DDoS e sequestro de dados de 223 milhões de brasileiros.
- Grupo Ultra é alvo de *ransomware*.

Fev
- Criminoso anunciou venda de informações da CPFL Energia.
- *Hacker* tenta envenenar água na Florida.

Mar
- Vulnerabilidade 0-day no Microsoft Exchange Server foi divulgada.
- Divulgada vulnerabilidades na maioria das versões BIG-IP.

Abr
- TJ:RS foi vitima de *ransomware.*

Mai
- Ataque de *hackers* a maior óleoduto dos EUA fez governo declarar estado de emergência.
- JBS é vitima de *ransomware*.

Jun
- O Grupo Fleury ficou com sistema fora do ar por uma semana.
- Electronic Art sofreu ataque e teve dados da FIFA e Frostbite roubados

Jul
- Sistema de trens e o governo do Irã são interrompidos após ataque.
- Kaseya VSA sofreu ataque de *ransomware.*

Ago
- Lojas Renner foi vitima de *ransomware.*
- Gigabyte Technology foi vitima de *ransomware.*

Set
- *Hackers* vazam senhas de 500 mil contas de VPN da Fortinet

Out
- Código-fonte do sistema do Enem foi vazado.
- Invasão *hacker* rouba dados de toda população Argentina.

Nov
- Unicred, Atento, CVC e Porto Seguro sofreram ataques.
- Violação de segurança da GoDaddy expõe dados de usuários do WordPress

Dez
- Grupo LAPSUS$ ataca Ministério da Saúde e outros órgãos do Governo.
- Apex Brasil foi vitima de *ransomware*.

Fonte: Brasscom, brasscom.org.br/pdfs/seguranca-da-informacao/, Instituto igarapé, 2021, Apura Cyber Intelligence, 2021.

Rol Exemplificador de Ataques Cibernéticos

Os ataques correspondem a qualquer ação que comprometa a segurança da organização. Quando um ataque é bem-sucedido causa dano de diversas magnitude à organização.

Exemplos de técnicas que geram vulnerabilidades

- **Engenharia Social:** Uma tentativa de induzir alguém a revelar informações (por exemplo, uma senha) que podem ser usadas para atacar sistemas ou redes.
- ***Phishing***: Uma técnica para tentar adquirir dados confidenciais, como números de contas bancárias, por meio de uma solicitação fraudulenta por *e-mail* ou em um *site*, na qual o criminoso se disfarça de empresa legítima ou pessoa respeitável.
- **Ataques de Força Bruta:** Utiliza criptoanálise para buscar exaustivamente a descoberta de senhas nos mais variados meios tecnológicos, *web*, servidores, ativos de rede etc.
- ***Fake News***: O compartilhamento de *fake news* e os processos de desinformação são pontos chave no cenário atual de ataques digitais.

Exemplos de técnicas que exploram as falhas

- **Negação de Serviço (DoS e DDoS)**: Interrompe um serviço, um ou mais computadores conectado à internet, com a geração de sobrecarga no processamento do computador alvo ou no tráfego de dados da rede à qual o alvo está conectado.
- ***Pharming***: Usar meios técnicos para redirecionar os usuários para acessar um site falso disfarçado de legítimo e divulgar informações pessoais.
- **IP *Spoofing***: Falsificar o endereço de envio de uma transmissão para obter entrada ilegal em um sistema seguro.
- ***Malware***: Programas maliciosos que se infiltra e obtém controle sobre um sistema de computador ou dispositivo móvel para roubar informações valiosas ou danificar dados, tais como: vírus, cavalos de tróia, *adware*, *spyware*, *backdoors*, *keyloggers*, *worms*, *bots* e *rootkits*.
- **SIM *Jacking***: O criminoso usa várias técnicas que geram vulnerabilidade, geralmente engenharia social, para transferir o número de telefone da vítima para o seu próprio cartão SIM com objetivo de redefinir as senhas ou receber códigos de verificação e acessar contas protegidas

Nota: Existem outros tipos de técnicas de ataques e que estão constantemente se sofisticando e sofrendo modificações.

Fonte: Brasscom, NIST (https://csrc.nist.gov/glossary) ; Europol, 2020; Mascarenha Neto e Junqueira. Segurança da Informação: Uma visão sistêmica para implantação em organizações 2019;

Definições

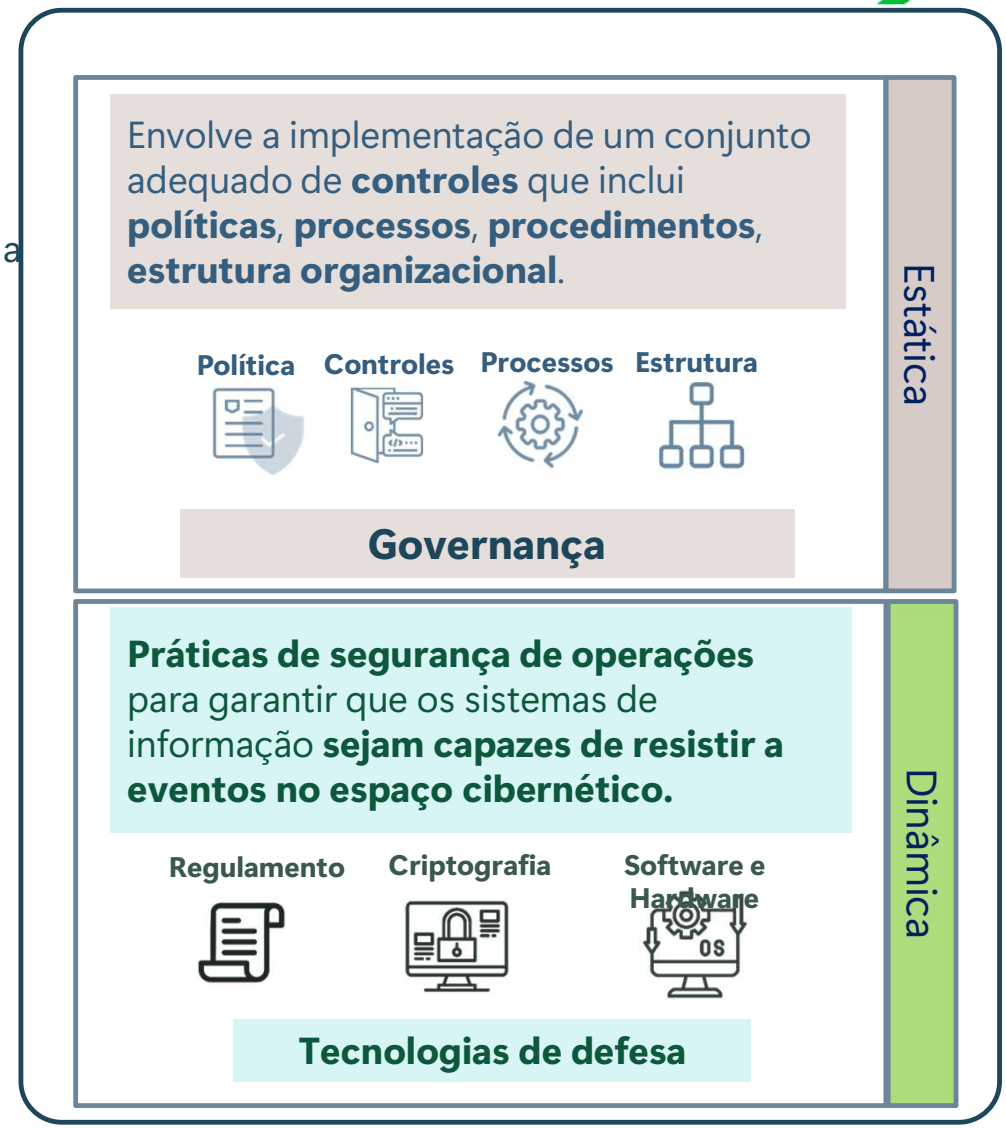
A definição presente no **Glossário do Gabinete de Segurança Institucional (GSI) – Brasil:**

Segurança Cibernética: Ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis;

Segurança da Informação: Ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

Sérgio Paulo Gallindo
Presidente da Brasscom

*"Eu costumo falar com muitos que eu entendo a **segurança da informação** como tendo **duas abordagens:** uma abordagem que eu chamaria de **estática**, que comporta a **gestão de risco**, proteção perimetral e a higidez de todo o ambiente; e outra, que eu chamo de **dinâmica**, que é o **combate aos incidentes**."*



 Fonte: Brasscom, GSI, 2021; Governo Digital, 2021; Anatel, 2021

Gestão de Risco

A **Gestão de Risco** visa **conter e prevenir a possibilidade de impactos negativos** sobre objetivos pretendidos, caso alguns dos riscos avaliados venham a se concretizar. Portanto, o **gerenciamento de riscos** objetiva **reduzir ao mínimo possível os impactos dos riscos sobre a própria organização e terceiros**, com a adoção de melhores práticas de infraestrutura, políticas e metodologias, tendo em mente a tecnologia disponível; o custo de implementação; a natureza, escopo, contexto e finalidade das atividades de processamento do controlador de dados; e a probabilidade e magnitude dos riscos envolvidos.

Considerando a ampla variedade de tratamento de dados realizados por diferentes tipos de organizações, é importante manter uma flexibilidade em torno da metodologia de análise de risco de modo que as especificidades de cada organização e da natureza dos dados que ela trata possam ser ponderados como parte desse processo de avaliação. Nesse sentido, **as organizações podem se basear nas diversas metodologias de avaliação e gerenciamento de risco existentes e que melhor respondem aos seus modelos de negócios.**

- **Avaliação de risco:**
  A **ENISA** define a avaliação de risco como um processo científico e tecnológico composto por três etapas: identificação de riscos, análise de risco e avaliação de risco . O escopo da avaliação é coordenar o uso de recursos e monitorar, controlar e minimizar a probabilidade e/ou o impacto de eventos infelizes que possam colocar em risco a informação de interesse para a segurança da sociedade e do Estado.

- **Gerenciamento de risco:**
  O **NIST** diz que o gerenciamento de riscos é o processo contínuo de identificação, avaliação e resposta ao risco. Para gerenciar riscos, as organizações, públicas ou privadas, devem entender a probabilidade de um evento ocorrer e o impacto resultante. Com esta informação, podem determinar o nível aceitável de risco para a entrega de serviços e sua tolerância ao risco. Com uma compreensão da tolerância ao risco, pode haver priorização das atividades de segurança da informação e/ou segurança cibernética, permitindo que decisões conscientes sobre os gastos com segurança da informação e/ou segurança cibernética sejam tomadas.

Daniel Aviz
Gerente de Segurança da Informação
TOTVS

" (...) Entenda tudo aquilo que pode interferir no processo de geração de valor e comece sabendo quem são as ameaças do seu negócio, se a sua ameaça é um funcionário interno descontente, se a sua ameaça é um hacker, se a sua ameaça é um país; entenda quem pode ameaçar a prosperidade do seu negócio, se é um fraudador de sistema financeiro, se ele está interessado no dinheiro ou na informação e o que ele pode fazer com isso."

 Fonte: Brasscom, 2017; CPIL, 2014 ; CPIL, 2016.

Padrões de Segurança

NIST Privacy framework

Oferece um conjunto de ferramentas de uso voluntário para viabilizar uma estratégia de privacidade para as organizações que desejam aprimorar sua forma de utilizar e proteger os dados pessoais; também oferece detalhadamente explicações sobre conceitos de gerenciamento de risco.

Metodologia ENISA

Fornece um Inventário de Gestão de Riscos e Métodos e Ferramentas de Avaliação de Riscos e disponibiliza direcionamentos para melhorar a cibersegurança de pequenas e médias empresas e para estruturas críticas.

Ferramentas de *soft law* – Normas ISO

- **ISO 27001:2013** integra um conjunto de políticas, procedimentos e processos que formam o **Sistema de Gestão da Segurança e Informação**, uma estrutura central que permite às organizações adotar uma consistência para os seus exercícios de gestão de risco e segurança da informação.
- **ISO 27002** é um código de práticas com um conjunto completo de **controles** que auxiliam aplicação do **Sistema de Gestão da Segurança da Informação.**
- **ISO 27005:2018** sustenta os conceitos aplicados da ISO 27001 e delineia como as organizações podem **identificar os perigos** de segurança da informação**, priorizar suas maiores ameaças** e **selecionar um curso de ação** apropriado.
- **ISO 27701:2019** especifica os requisitos e fornece as diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um **Sistema de Gestão de Privacidade da Informação**, e funciona como extensão das normas **ISO 27001** e **ISO 27002**, para a gestão da privacidade dentro do contexto da organização.
- **ISO 31000:2018** apresenta um conjunto de diretrizes para a **gestão de riscos** enfrentados por quaisquer organizações.

Fonte: Brasscom, 2021;

Segurança da Informação nas empresas e usuários

A conscientização de que todos possuem papéis sejam da tecnologia, da indústria e dos indivíduos, é o primeiro passo rumo à confiança no ecossistema digital.

Boas práticas para dia-a-dia dos indivíduos:

- Escolha de senhas fortes;
- Nunca divulgue ou compartilhe senhas pessoais;
- Alteração periódicas de suas senhas;
- Preferencialmente não utilizar senhas iguais para serviços diferentes;
- Utilize a autenticação de dois fatores;
- Leia as políticas de privacidade e uso do aplicativo;
- Mantenha antivírus sempre atualizado e pleno funcionamento;
- Não ignore notificações sobre detecção de ameaça;
- Mantenha opção de backup ativada;
- Cuidado com redes de wi-fi não seguras;
- Não abrir e-mail de remetentes desconhecidos;
- Sempre verifique a URL dos sites que irá acessar;
- Não insira seus dados pessoais em sites duvidosos;
- Mantenha-se atualizado sobre boas práticas de segurança da informação.

Boas práticas para o desenvolvimento da Segurança da Informação nas empresas:

Identificar e mensurar as vulnerabilidades

Criar Métricas para verificar a resiliência do negócio, exemplo: "quanto tempo o site pode ficar fora do ar?"

Armazenamento da Informação para avaliar qual informação deverá ser mantida

Escolha da Segurança deve-se pautar na confiança, daquele parceiro que vai ser o melhor nos momentos de crise.

Maturidade, os responsáveis pela empresa devem trabalhar para conscientizar até o menor nível, e para isso deve haver,

Comunicação entre todos os funcionários, para que qualquer problema possa ser relatado e tratado.

Fonte: Brasscom, 2021

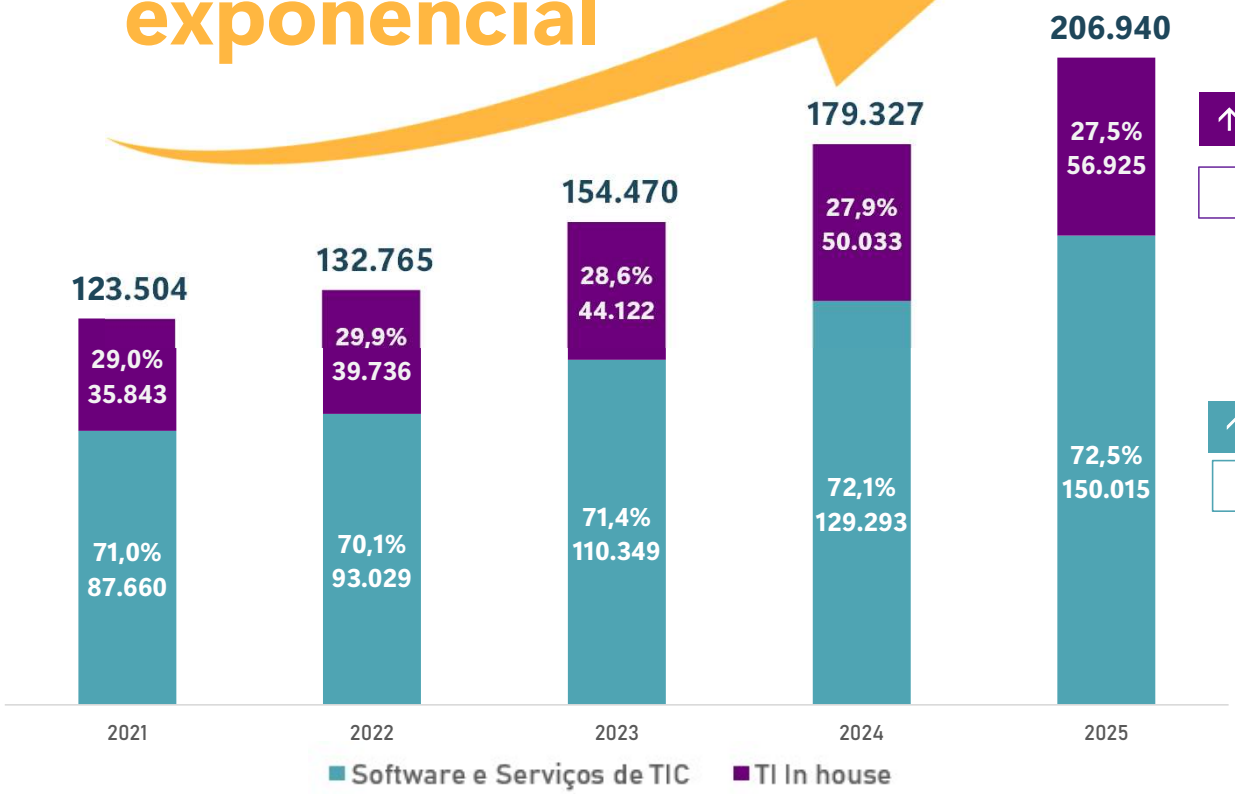
Demanda de novos talentos em tecnologia em **5 anos**

Brasscom

Crescimento exponencial

797 mil

Demanda total de **797 mil,** com uma média simples de **159 mil empregos por ano**.



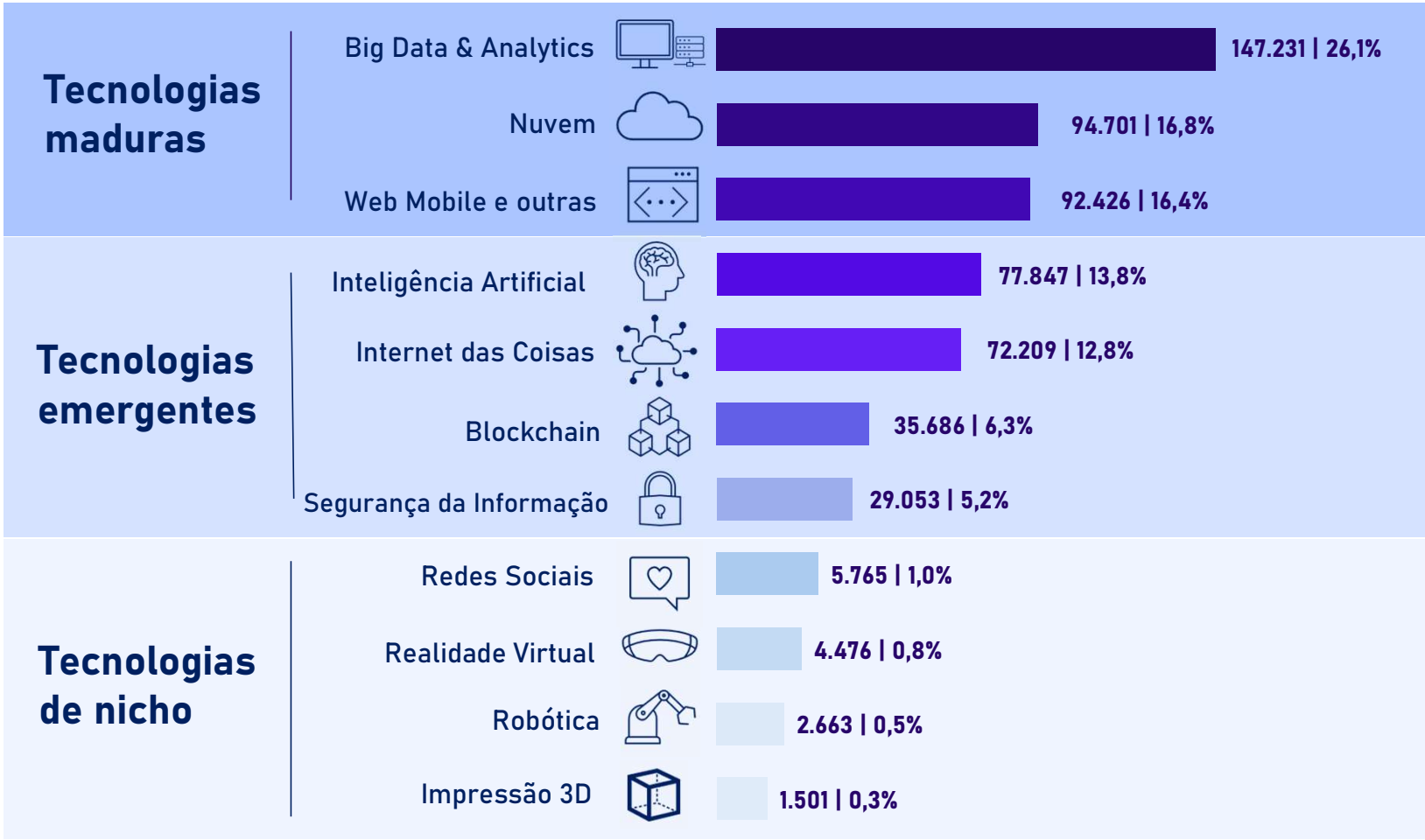
A remuneração média de TI In House[1] é de **R$ 5.784** sendo **3,2 vezes** maior que o salário médio nacional (em 2021-12)

A remuneração média de Software e Serviços de TIC é de **R$ 5.548** sendo **3,1 vezes** maior que o salário médio nacional (em 2021-12)

Nota: [1] TI In House tem a mesma remuneração se não maior que serviços de alto valor agregado.
[2] Essa projeção foi publicada em dezembro de 2021 com a análise dos dados de emprego até setembro de 2021. As novas contratações até dezembro de 2021 foram de 154.221, superando em 24,8% a projeção publicada de 123.504 para 2021.

Fontes: Brasscom, Bacen, IDC, Relatórios Financeiros das Estatais, RAIS e Caged, Novo Caged, Censo do Ensino Superior (INEP, 2019)

As **Tecnologias Maduras** vão ser as principais geradoras de empregos em **5 anos**



Fontes: Brasscom, World Economic Fórum (Future of Jobs - 2021), ABES (Mercado Brasileiro de software – Panorama e Tendências – 2021), Bacen, IDC, Relatórios Financeiros das Estatais, RAIS, Caged e Novo Caged.

Perfil do Profissional de Segurança da Informação

Os profissionais de SI são responsáveis pela administração de uma ampla variedade de sistemas de TI em toda a empresa.

Isso pode envolver a administração diária de ferramentas e dispositivos de segurança cibernética, bem como suporte de primeiro e segundo nível para informações de segurança e gerenciamento de eventos.

Para o desenvolvimento do profissional, é essencial um conhecimento prático de protocolos e ferramentas de rede.

Competências Gerais do Profissional

Brasscom

Gerenciar e operar a Segurança da Informação, desde a autorização e monitoramento de acesso a instalações ou infraestrutura de TI, até a conformidade com a legislação pertinente.

Auxiliar os usuários na definição de seus direitos e privilégios de acesso, bem como executar tarefas de administração de segurança não padrão e resolver problemas de segurança.

Garantir que os registros e segurança sejam precisos e completos e que as solicitações de suporte sejam tratadas de acordo com os padrões e procedimentos estabelecidos.

Monitorar a aplicação dos procedimentos de administração de segurança e analisar os sistemas de informação em busca de violações reais ou potenciais de segurança.

Auxiliar na resolução de problemas relacionados a controles de acesso e sistemas de segurança bem como garantir que todas as violações identificadas sejam completamente investigadas e que as alterações de segurança do sistema sejam implementadas.

Investigar violações de segurança e recomendar as ações necessárias. Manter os processos de administração de segurança e verificar se todas as solicitações de suporte são atendidas de acordo com os procedimentos acordados.

Interagir de perto com fornecedores de produtos provedores de serviços, com pessoal de vários outros departamentos De TI, negócios e administrativo.

Contribuir para a criação e manutenção de politicas, padrões, normas, processos documentações e diretrizes para segurança física e eletrônica dos sistemas.

Revisar novas propostas de negócios e fornecer consultoria especializada sobre questões e aplicações de segurança

22 **Fonte**: Brasscom, 2021

Currículo de Referência para Segurança da Informação

Os **Currículos de Referência** da **Brasscom** foram elaborados de acordo com a resolução do **Conselho Nacional de Educação** (CNE, 2020).

O **Currículo de Referência** em **Segurança da Informação** é baseado no cruzamento de informações dos cursos mais bem conceituado nos rankings acadêmicos, grandes empresas de mercado e pesquisas setoriais.

Estrutura do Currículo de Referência

- Perfil do Egresso;
- Competências Gerais;
- Princípios e Diretrizes Pedagógicas
- Perfil Curricular, Organização Curricular
- Sistemática de Avaliação
- Ementário
- Carga Horária
- Metodologias Ativas

Fonte: Brasscom, 2021, brasscom.org.br/pdfs/seguranca-da-informacao/

Organização do Currículo de Referência para Segurança da Informação

Brasscom

Eixo de Tecnologia da informação (520 horas)

Introdução à computação, Arquitetura e Organização de Computadores, Redes e Conectividade, Introdução à Segurança da Informação, Banco de Dados, Introdução à Programação, Fundamentos de Análise Quantitativa e Estrutura de Dados.

Eixo de Segurança Defensiva (440 horas)

Gestão de Riscos, Operações de Segurança, Gestão da identidade e Controle de Acesso (IAM), Segurança Proteção e Privacidade de Ativos, Gestão da Continuidade de Negócios, Modelagem de Ameaças.

Eixo de Segurança Ofensiva (220 horas)

Gestão, Avaliação e Mitigação de Vulnerabilidades, Comunicação e Segurança de Rede, Avaliação e Testes de Segurança.

Eixo de Desenvolvimento Seguro (260 horas)

Criptografia Aplicada, Segurança e Desenvolvimento de Software, Arquitetura e Engenharia de Segurança

Sistema de avaliação

O processo avaliativo precisa ser:

Constante

Deve estar inserido na relação planejamento, ensino e aprendizagem.

Diverso

A avaliação deve ser materializada por meio de uma diversidade de instrumentos avaliativos.

Democrático

O processo avaliativo precisa ser apresentado no começo de cada disciplina, discutido e negociado com os estudantes.

Pertinente

Considera o componente curricular, o conteúdo trabalhado e os objetivos de aprendizagem do curso.

Quanto aos instrumentos de avaliação, estes se caracterizam pelos momentos e artefatos utilizados para coleta de dados que subsidiam a avaliação.

Fonte: Brasscom, 2021, brasscom.org.br/pdfs/seguranca-da-informacao/

Instrumentos de avaliação

Resolução de problemas reais:

Exigindo as competências técnicas, cognitivas e socioemocionais das disciplinas do período.

Prova individual ou emprego (com e sem consulta):

Além da compreensão dos conceitos, com estudos de casos para avaliar o saber fazer.

Estudos de Casos:

Contextualização e desafios para solucionar.

Seminários:

Importantes para que sejam avaliados competências como comunicação, assertividade, organização do grupo, liderança, etc.

Autoavaliação:

É uma das prerrogativas das competências socioemocionais, coloca o estudante como protagonista no gerenciamento da sua aprendizagem(aprender a aprender);

Trabalhos em grupos:

Essencial para o desenvolvimento de competências requeridas no trabalho colaborativo e digital.

Além das avaliações formativas recomenda-se processos para diagnose do conhecimento de estudantes no inicio do processo de aprendizagem e as somativas ao termino de cada ciclo de conhecimento.

Desafio de formação em TIC e introdução da estratégia

A oferta de **53 mil** formandos ao ano é insuficiente para atender os **159 mil** profissionais demandados ao ano até 2025

A inoculação tecnológica é uma abordagem para potencializar a empregabilidade dos egressos das formações em TCEM no setor de tecnologia.

Consiste na oferta de disciplinas eletivas que capacitem os alunos nas tecnologias em alta demanda pelo setor de TIC.

Oferta
53 mil
Formados ao ano com perfil tecnológico no Ensino Superior

<

Demanda
159 mil
Profissionais demandados média simples ao ano (2021-2025)

Estratégia ∑TCEM
Inoculação tecnológica nos cursos de Ciências, Engenharia e Matemática para aumento da oferta de profissionais

Oferta Potencial
237 mil
Formados ao ano em $\sum TCEM$

>

Demanda
159 mil
Profissionais demandados média simples ao ano (2021-2025)

Fontes: Brasscom, Bacen, IDC, Relatórios Financeiros das Estatais, RAIS e Caged, Novo Caged, Censo do Ensino Superior (INEP, 2019)

Afinidade e Inoculação Tecnológica

Afinidade

Afinidade é a característica das grades curriculares ofertadas pelas instituições de ensino que oferecem formação em TCEM, que têm superposição com tecnologia.

A Brasscom desenvolveu um Índice de Afinidade (de 0 a 5) para avaliar o grau de Afinidade entre as grades curriculares ofertadas e a demanda de talentos em programação.

Foram analisadas 406 grades curriculares.

$$\textit{Índice de afinidade} = \frac{\sum \textit{Número de grades curriculares} \times \textit{Peso correspondente}}{\textit{Total de grades curriculares dos cursos}}$$

Inoculação Tecnológica

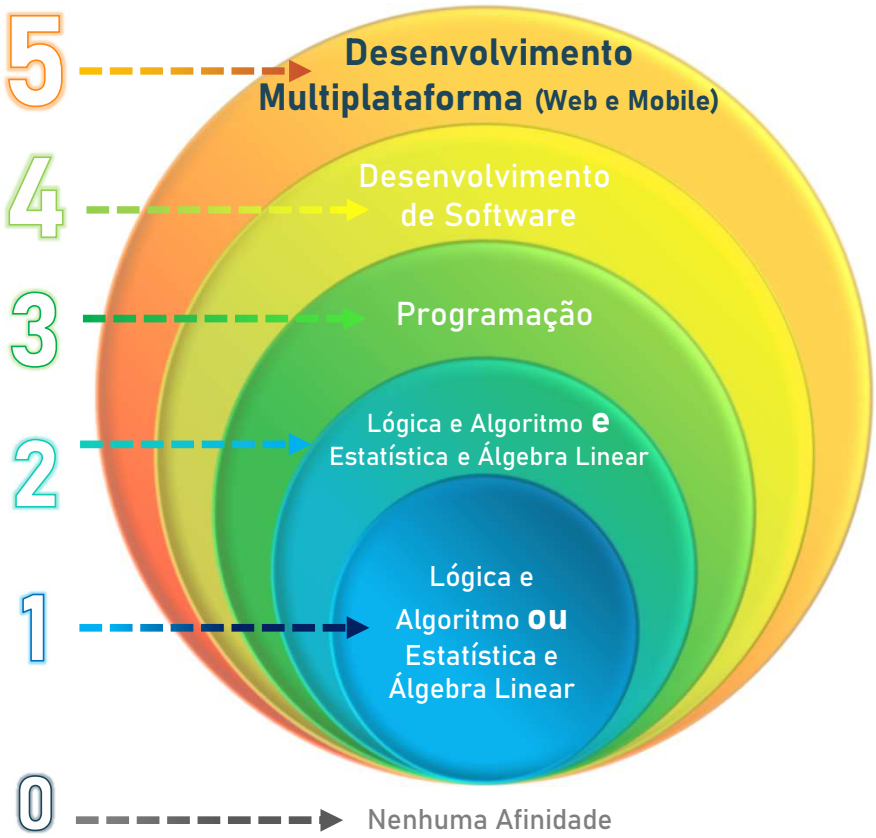
A inoculação tecnológica é uma abordagem para potencializar a empregabilidade dos egressos das formações em TCEM no setor de tecnologia.

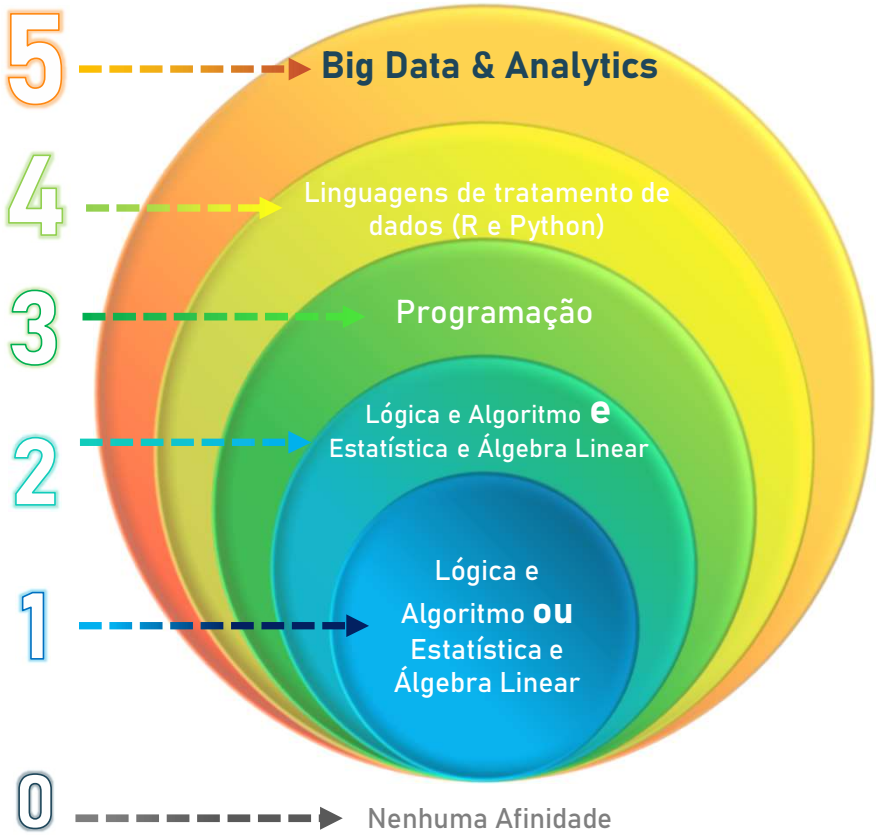
Consiste na oferta de disciplinas eletivas que capacitem os alunos nas tecnologias em alta demanda pelo setor de TIC.

O grau de inoculação é inversamente proporcional à afinidade, ou seja, quanto menor a afinidade, maior o grau de inoculação tecnológica.

A Inoculação Tecnológica pode ser usada para outras áreas de conhecimento, tais como, inteligência artificial, nuvem e segurança da informação

A **Afinidade** pode ser aferida em relação com a principal tecnologia almejada na formação, tais como, Desenvolvimento Multiplataforma (Web e Mobile) ou Big Data & Analytics

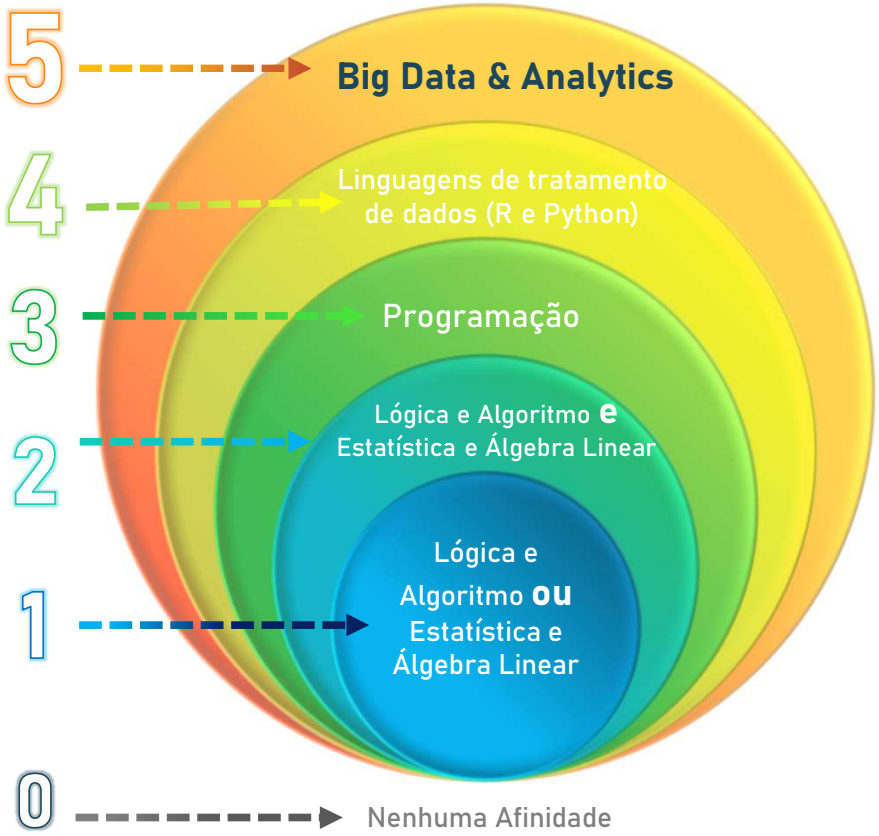




Nota: (1) A presença das disciplinas de Lógica e Algoritmo ou de Estatística e Álgebra Linear já é suficiente para classificar o curso com o peso 1. Para ser classificado com o peso 2, é necessária a presença simultânea de ambas disciplinas, Lógica e Algoritmo e Estatística e Álgebra Linear.
(2) Programação refere-se ao aprendizado de uma linguagem de programação, Desenvolvimento de Software engloba o ensino de metodologias ágeis e de *design thinking* e UX

Inoculação Tecnológica para Big Data & Analytics

Afinidade



Inoculação Tecnológica

- Big Data e Analytics
- Big Data e Analytics
  Linguagens de tratamento de dados (R e Python)
- Big Data e Analytics
  Linguagens de tratamento de dados (R e Python)
  Programação
- Big Data e Analytics
  Linguagens de tratamento de dados (R e Python)
  Programação
  Estatística e Álgebra Linear **ou** Lógica de programação e Algoritmo
- Big Data e Analytics
  Linguagens de tratamento de dados (R e Python)
  Programação
  Estatística e Álgebra Linear **e** Lógica de programação e Algoritmo

Perspectivas de mercado para Segurança da Informação em 2022

Ajustes nas práticas de Segurança Cibernética em ambientes de nuvem será um dos principais **desafios** dos gestores de TI.

57% das empresas afirmam que contarão com **apoio externo** focado em gerenciar e operar ambientes com soluções de segurança mais modernas.
Os serviços de segurança totalizarão quase **US$ 1B** no Brasil, enquanto que as **soluções de segurança, em hardware ou software**, superarão **US$ 860M.**

A **otimização** das práticas de **segurança de gestão** e **proteção dos dados** receberá maior atenção das lideranças.

O **5G** no Brasil movimentará **US$ 25,5B** até **2025** e impulsionará diversas tecnologias, inclusive tecnologias de segurança.

Melhoria da segurança compõem os **principais KPIs de avaliação** de sucesso nas implementações de IoT pelas organizações.

Fonte: Brasscom; IDC (Black Book 3ª Plataforma, 2021 H1); IDC- Predictions, 2022

Obrigado!

brasscom.org.br

Siga-nos nas redes sociais