

Guia prático

31 dicas de cibersegurança

dadas por 31 executivos da Accenture Security, para o dia a dia de quem trabalha, compra, viaja e vive online.

Accenture Security

Sobre este guia

31 dias.
31 executivos.
31 dicas.

No Mês da Conscientização em Cibersegurança, em outubro de 2026, 31 executivos da Accenture Security gravaram, um por dia, um vídeo curto com uma dica para o dia a dia. Este guia reúne todas elas, organizadas pelas etapas de um ataque, para você consultar quando quiser.

31
dias de dicas

31
executivos

31
dicas práticas

5
etapas de um ataque

Como usar este guia

Veja o caminho

O infográfico mostra as etapas de um ataque e as barreiras que o interrompem.

Ache sua dica

Use o sumário para ir direto ao assunto que importa para você.

Assista ao vídeo

Cada dica traz o link para o vídeo do executivo que a gravou.

Pare. Pense. Confirme.

A ideia que atravessa as 31 dicas: antes de clicar, atender ou compartilhar, faça uma pausa e verifique.

Sumário

Isca 6

Phishing: pare antes do clique 7
Urgência pode ser armadilha 7
Cuidado com o QR Code 7
Pendrive achado: não conecte 8
Vaga boa demais? Desconfie 8
Compras online: promoção ou golpe? 8

Invasão 9

Senha forte e fácil de lembrar 10
Uma conta, uma senha 10
Segundo fator: a segunda trava 10
Aprovação que você não pediu: negue 11
Wi-Fi grátis, risco real 11
Deepfake: ver e ouvir não é crer 11

Acesso 12

Cuide dos acessos, humanos e digitais 13
Acesso demais, risco demais 13
Segregação de funções: ninguém faz tudo 13
Saiu da mesa? Bloqueie a tela 14
Revise antes de enviar 14
Reunião online: proteja tela e sala 14

Impacto 15

Atualizar fecha portas 16
Proteja o que não tem suporte 16
SAP desatualizado, risco invisível 16
Ataque em OT: prepare o time 17
Q-Day: a criptografia em xeque 17
Dados e IA pública: antes do Enter, pense 17

Resposta 18

Resposta rápida a incidentes 19
Depois do incidente: aprender 19

No centro de tudo 21

Pare, olhe e verifique 22
60 segundos antes de agir 22
Saiba o que proteger 22
IA: defesa e ataque 23
Segurança também é cultura 23

Sobre a Accenture 24

Prefácio

A tecnologia ajuda, mas o que sustenta a segurança é a decisão certa, no momento certo



No Mês da Conscientização em Cibersegurança, 31 executivos da Accenture Security abriram espaço na agenda para gravar um vídeo curto, um por dia, com uma dica prática para o dia a dia. Cada um falou do assunto que conhece de perto, de golpes do cotidiano à computação quântica.

Para quem vê de fora, foram 31 vídeos. Para nós, foi um retrato de um dia comum na Accenture Security: proteger ambientes críticos, responder a incidentes, priorizar o que importa para o negócio e ajudar as pessoas a decidirem melhor.

Este guia nasceu para que essas dicas não fiquem restritas a um mês. Aqui, elas estão reunidas e organizadas pelas etapas de um ataque, com o vídeo de cada executivo a um clique de distância. Use, consulte e compartilhe com a sua família, os seus amigos e o seu time. Quem está perto de você também precisa dessas informações.

Se uma ideia atravessa todas as dicas, é esta: antes de clicar, atender ou compartilhar, pare, pense e confirme.

Obrigada a cada executivo que compartilhou o que sabe, e a você, por levar essa conversa adiante.

Um abraço,

Vanessa Fonseca

Cybersecurity Lead Latam, Managing Director at Accenture

O caminho de um ataque e as 31 barreiras que o interrompem

Cada etapa de um ataque tem dicas que ajudam a barrá-lo. Clique em uma delas para ir direto ao conteúdo.

Isca

A mensagem, o link ou o QR Code que chama a atenção

- Phishing
- Urgência
- QR Code
- Pendrive
- Falso emprego
- Compras online

Invasão

A porta de entrada: senhas, segundo fator e atenção

- Senha forte
- Uma senha por conta
- Segundo fator
- Aprovação indevida
- Wi-Fi público
- Deepfake

Acesso

Quem pode fazer o quê, dentro de casa

- Gestão de acessos
- Acesso demais
- Segregação de funções
- Bloqueio de tela
- E-mail
- Reunião online

Impacto

Onde o ataque dói: sistemas, ambientes e dados

- Atualizações
- Legado sem suporte
- SAP
- OT
- Q-Day
- IA pública

Resposta

O que fazer quando algo dá errado

- Resposta a incidentes
- Lições aprendidas

No centro de tudo

Pessoas, o básico bem feito e a IA como aliada

- Pare, olhe e verifique
- 60 segundos
- O que proteger
- IA
- Cultura



Etapa 1 de 5

Isca

O ataque começa com uma isca: uma mensagem, um link, um QR Code, uma vaga boa demais para ser verdade.

- Phishing
- Urgência
- QR Code
- Pendrive
- Falso emprego
- Compras online



Fabio Araujo
Cybersecurity Senior Manager at Accenture

Assistir ao vídeo

Phishing: pare antes do clique

Phishing é a tentativa de enganar você com mensagens e e-mails falsos para roubar senhas, dados ou informações da empresa. Um único clique pode comprometer uma conta e abrir caminho até um ransomware.

Faça assim

Desconfie de urgência, links estranhos e pedidos inesperados de senha ou código. Pare, confira e valide.



Waleria Duarte
Gerente Comercial na Accenture

Assistir ao vídeo

Urgência pode ser armadilha

O atacante só precisa de uma decisão tomada no automático: um link clicado sem pensar, um pedido urgente não confirmado, uma informação compartilhada no impulso. A urgência é uma ferramenta poderosa da engenharia social.

Faça assim

Quando algo parecer urgente, inesperado ou fora do padrão, desacelere: pare, pense e confirme.



Juliana Girasol
Cyber Security Associate Director at Accenture

Assistir ao vídeo

Cuidado com o QR Code

QR Codes estão em cardápios, estacionamentos, eventos e até placas de rua. Criminosos os transformam em códigos maliciosos que levam a páginas feitas para roubar dados pessoais, bancários e credenciais.

Faça assim

Se você não conhece a origem do QR Code, não escaneie.



Fernando Sao Pedro
Security Transformation Associate Director at Accenture

Assistir ao vídeo

Pendrive achado: não conecte

Dispositivos esquecidos no metrô, no ônibus ou no shopping, enviados como brinde ou que aparecem no escritório são uma estratégia de ataque que explora a curiosidade. Em segundos, podem abrir espaço para malware e roubo de dados.

Faça assim

Se não conhece a origem, não conecte. Se achar um dispositivo suspeito, avise o time de segurança ou o suporte de TI.



Saint'Claire Mesquita
CISO, Chief Information Security Officer at Accenture

Assistir ao vídeo

Vaga boa demais? Desconfie

No golpe do falso emprego, alguém diz que você foi selecionado para uma grande oportunidade. Os sinais de alerta: aplicativo fora das lojas oficiais, apelo de urgência e salário ou benefícios altos demais.

Faça assim

Nunca passe senhas ou códigos, nem envie biometria e documentos sem validar a empresa. Não instale apps fora das lojas oficiais.



Carlos Eduardo F. Pessanha
Security Delivery Manager at Accenture

Assistir ao vídeo

Compras online: promoção ou golpe?

Ofertas incríveis em redes sociais e anúncios podem esconder golpes, e golpistas também pagam para divulgar lojas falsas. Nem todo mundo tem a mesma relação com o ambiente digital, então vale ajudar quem está perto de nós.

Faça assim

Desconfie de preço muito baixo, confira o site e a reputação da loja, veja o nome de quem recebe o Pix, use cartão virtual e nunca ignore alertas do banco.



Etapa 2 de 5

Invasão

Quem cai na isca ainda precisa passar pela porta de entrada. Senhas, segundo fator e atenção fecham esse caminho.

- Senha forte
- Uma senha por conta
- Segundo fator
- Aprovação indevida
- Wi-Fi público
- Deepfake



Helvio Junior
Cybersecurity
Manager at Accenture

Assistir ao vídeo

Senha forte e fácil de lembrar

Nos testes de invasão, as senhas vêm de credenciais vazadas, reaproveitadas em vários sites, e de senhas fracas ou previsíveis, como 123456. Um único deslize pode custar milhões.

Faça assim

Use uma senha longa (como uma estrofe de música de que você gosta), uma senha única por site, um gerenciador de senhas e autenticação multifator.



Nadia Premici
Cyber Security Senior
Manager at Accenture

Assistir ao vídeo

Uma conta, uma senha

Quando uma conta é comprometida, criminosos testam a mesma senha no e-mail, nas redes sociais, em aplicativos financeiros e até em sistemas corporativos.

Faça assim

Use uma senha diferente para cada acesso, de preferência frases longas, com gerenciador de senhas e autenticação multifator.



Emerson Moraes
Sales Director,
Security at Accenture

Assistir ao vídeo

Segundo fator: a segunda trava

Os atacantes buscam credenciais, usuário e senha, e muitas já vazaram. Com o segundo fator de autenticação, a senha vazada sozinha não abre a porta, e você ainda recebe um alerta da tentativa de acesso.

Faça assim

Habilite o segundo fator no WhatsApp, no e-mail e nas plataformas que você usa. Leva cerca de 5 minutos.



Alysson Maciel
Security Transformation Senior Manager at Accenture

Assistir ao vídeo

Aprovação que você não pediu: negue

Receber um código ou uma notificação de segundo fator que você não solicitou é um alerta: o atacante já passou pela sua senha. Ele ganha confiança fingindo ser o suporte de TI ou do banco e cria urgência para obter o código.

Faça assim

Se isso acontecer, desligue, procure um canal seguro, redefina a senha e avise a empresa ou o aplicativo.



Rogerio Pizi
Security Delivery Manager at Accenture

Assistir ao vídeo

Wi-Fi grátis, risco real

Golpistas criam redes com nomes parecidos com os de aeroportos, cafés e hotéis para espionar senhas, mensagens e dados bancários.

Faça assim

Prefira o 4G ou 5G do celular. Se precisar de Wi-Fi público, confirme o nome oficial da rede e evite senhas importantes, banco e compras.



Ivan Soares Cano
Senior Manager, Cybersecurity Transformation at Accenture

Assistir ao vídeo

Deepfake: ver e ouvir não é crer

Um pequeno trecho da sua voz pode bastar para reproduzir a sua fala. Ligações em silêncio e áudios com a voz do chefe ou de um familiar pedindo algo com urgência podem ser deepfake.

Faça assim

Pare, questione e confirme sempre por outro canal.



Etapa 3 de 5

Acesso

Dentro de casa, quem pode fazer o quê? Acessos, telas, e-mails e reuniões também são barreiras.

- Gestão de acessos
- Acesso demais
- Segregação de funções
- Bloqueio de tela
- E-mail
- Reunião online



Felipe Cruzeiro
Associate Director
at Accenture

Assistir ao vídeo

Cuide dos acessos, humanos e digitais

A grande ameaça pode estar dentro da empresa: quem saiu e continua com acesso, senha compartilhada, excesso de permissões e agentes de IA acessando sistemas sem gestão. Segurança é também comportamento, atitude e cultura.

Faça assim

Remova o acesso de quem saiu, dê um acesso por pessoa e só as permissões necessárias. Pergunte quem controla os agentes de IA.



Rafael Aosaki
Security Senior
Manager at Accenture

Assistir ao vídeo

Acesso demais, risco demais

Acessos que ninguém usa geram custo de licença todo mês, como no modelo de licenciamento por FUE do SAP, além de custo de monitoramento e de risco. É como pagar IPVA e seguro de um carro parado. O pior cenário é um acesso crítico nas mãos de quem nunca foi treinado.

Faça assim

Revise quem tem acesso a quê e questione acessos pedidos sem critério.



Lívia Muto Sciência
Security Delivery
Manager at Accenture

Assistir ao vídeo

Segregação de funções: ninguém faz tudo

Muitos dos maiores riscos vêm de acessos excessivos ou mal controlados, e não de invasões externas. A regra é simples: quem executa não pode ser quem aprova, como um cofre de banco com duas chaves em mãos diferentes.

Faça assim

Pergunte ao seu time: alguém consegue fazer um processo do começo ao fim sozinho? Se sim, vale revisar.



Julio Carvalho
Managing Director,
Cybersecurity at Accenture

Assistir ao vídeo

Saiu da mesa? Bloqueie a tela

Mesmo sozinho. A vulnerabilidade MouseJack, em receptores de mouse e teclado sem fio, permite que alguém a até 100 metros envie comandos e extraia arquivos e senhas. Um ataque via Bluetooth pode até simular um teclado pareado.

Faça assim
Sempre que sair da frente do computador, bloqueie a tela, em casa ou no escritório.



Wilson Costa
Security Delivery Senior
Manager at Accenture

Assistir ao vídeo

Revise antes de enviar

Um e-mail enviado para o destinatário errado pode expor dados sensíveis. Uma pausa de poucos segundos evita erros e protege as informações da empresa e dos clientes.

Faça assim
Confirme os destinatários, revise o anexo ou link e aplique o rótulo de sensibilidade. Se errar o envio, avise o canal de segurança na hora.



Thais Novaes
Security Transformation
Manager at Accenture

Assistir ao vídeo

Reunião online: proteja tela e sala

Em lugares públicos, posicione a tela onde passe pouca gente atrás de você e baixe o brilho. Convites abertos para qualquer pessoa com o link podem expor informações sensíveis.

Faça assim
Restrinja o acesso a quem foi convidado e use a sala de espera para filtrar quem entra.



Etapa 4 de 5

Impacto

Onde o ataque dói: sistemas desatualizados, ambientes críticos e dados que vazam para a IA pública.

- Atualizações
- Legado sem suporte
- SAP
- OT
- Q-Day
- IA pública



Lucas Teixeira
Security Delivery Manager at Accenture

Assistir ao vídeo

Atualizar fecha portas

Um ataque costuma começar com um clique, mas o estrago depende de uma brecha ainda não corrigida. Atualizar não impede o clique errado, mas impede que ele tenha consequências piores.

Faça assim
Atualize celular, navegador e notebook, e não adie o aviso. É o básico bem feito, e de graça.



Maycon Oliveira dos Santos
Service Delivery Manager at Accenture

Assistir ao vídeo

Proteja o que não tem suporte

Sistemas legados, sem suporte do fabricante, sustentam operações críticas, e a infraestrutura teme mexer neles. Manter esse "jabuti na árvore" deve ser uma decisão conjunta de infraestrutura e segurança, com controles compensatórios.

Faça assim
Se o jabuti não pode sair da árvore agora, proteja em camadas tudo o que está ao redor dele.



Aline Barreiros
Security Senior Manager, Platform/SAP at Accenture

Assistir ao vídeo

SAP desatualizado, risco invisível

Ambientes desatualizados não são só uma questão operacional. Acessos acumulados por quem mudou de área, ou de fornecedores com aprovação falha, passam despercebidos até aparecerem no financeiro ou na auditoria.

Faça assim
Revise o provisionamento, os riscos e os perfis de acesso SAP. Cibersegurança também é cultura, processo e controle interno atualizado.



Rodrigo Correia
Security Delivery Manager at Accenture

Assistir ao vídeo

Ataque em OT: prepare o time

O time do chão de fábrica, com operadores de painel e plantonistas de automação e manutenção, está pronto para identificar e responder a uma ameaça? Em infraestruturas críticas, cada minuto é crucial.

Faça assim

Estabeleça processos e treine o time da operação para identificar e responder a incidentes.



Antonio Horta, DSc
Cyber.AI Consulting Lead LATAM, Security Transformation Sr Manager at Accenture

Assistir ao vídeo

Q-Day: a criptografia em xeque

Está cada vez mais próximo o dia em que a computação quântica poderá quebrar a criptografia que conhecemos, o chamado Q-Day. Dados capturados hoje podem ser decifrados no futuro.

Faça assim

Comece a discutir o tema agora, antes que o Q-Day chegue e seja tarde demais.



Viviane Vargas
Sales Effectiveness Manager for Digital Core and Cybersecurity at Accenture

Assistir ao vídeo

Dados e IA pública: antes do Enter, pense

Um simples prompt também pode representar um risco. Dados de clientes, documentos internos, estratégias e propostas não devem ser inseridos em ferramentas públicas de IA.

Faça assim

Se você não publicaria aquela informação na internet, não a coloque em uma IA pública.



Etapa 5 de 5

Resposta

Quando algo dá errado, o que fazer nos primeiros minutos e como aprender com o que aconteceu.

- Resposta a incidentes
- Lições aprendidas



Wellington Pereira

Security Delivery Senior Manager, Crisis Response & Intel at Accenture

Assistir ao vídeo

Resposta rápida a incidentes

Incidente é quando alguém acessa, bloqueia, altera ou rouba informações sem autorização. Na hora, o nervosismo leva a decisões precipitadas, e por isso vale ter um checklist simples do que fazer e do que não fazer.

Faça assim

Se suspeitar que um computador foi afetado, desconecte-o da rede e da internet e evite desligá-lo na hora. Não enfrente sozinho: procure quem entenda do assunto.



Gabriela Rudge

Security Transformation Manager at Accenture

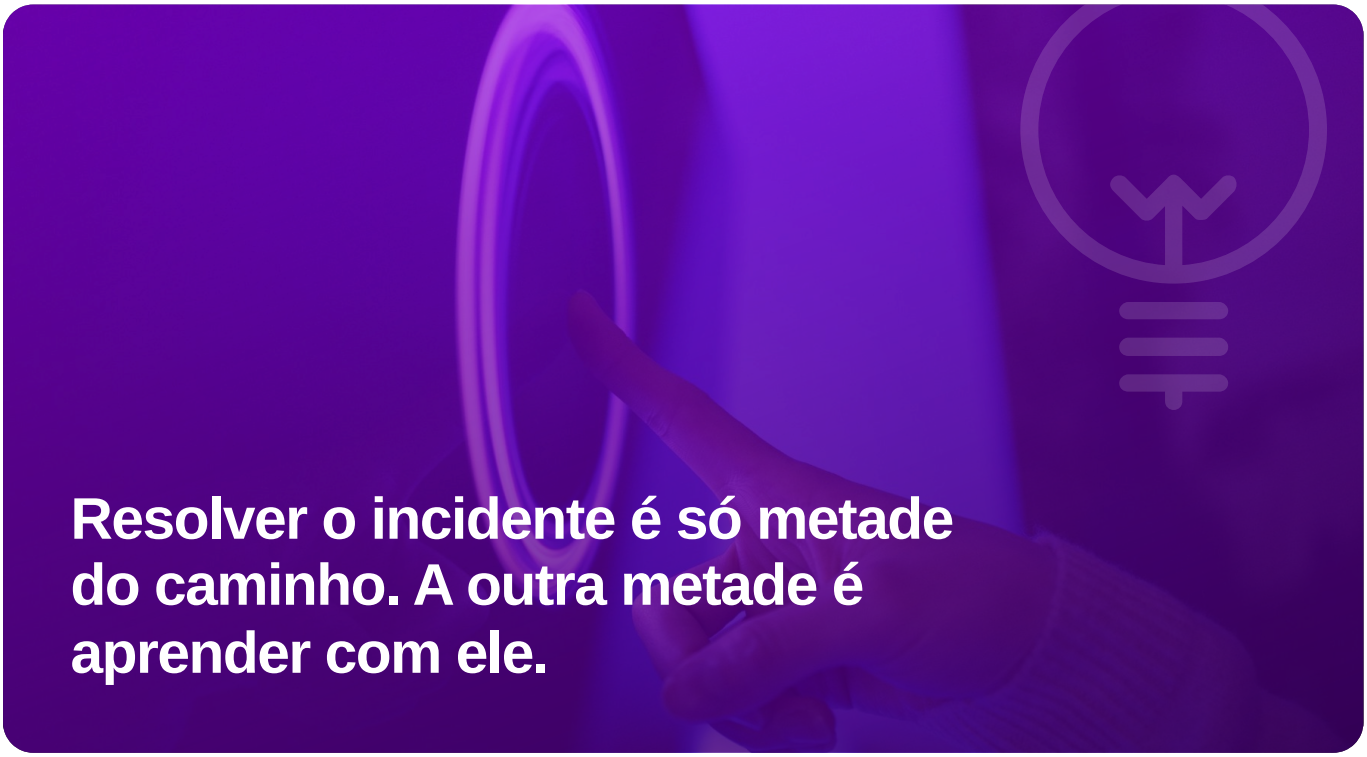
Assistir ao vídeo

Depois do incidente: aprender

Controlar o incidente e recuperar os sistemas não encerra o assunto. O processo de lessons learned transforma o aprendizado da resposta em ações que fortalecem a organização.

Faça assim

Além de perguntar "já resolvemos?", pergunte o que aprendemos e o que vamos fazer daqui para frente.



Para ter à mão

Se algo deu errado: primeiros passos



Na hora do susto, o nervosismo leva a decisões precipitadas. Por isso, vale ter um checklist simples do que fazer, reunido com o que os executivos recomendaram.



Caiu em um golpe financeiro

- Abra um boletim de ocorrência.
- Conteste a fraude com a instituição financeira.
- Troque senhas e códigos, começando pelo e-mail.
- Guarde todas as informações do contato com o golpista.
- Se enviou biometria ou documentos, busque ajuda jurídica.



Aprovou ou passou um código sem querer

- Desligue e procure um canal seguro.
- Redefina a senha.
- Avise a empresa ou o aplicativo.



Suspeita que um computador foi afetado

- Desconecte-o da rede e da internet.
- Evite desligá-lo na hora, para não perder informações.
- Não enfrente sozinho: procure quem entenda do assunto.



Enviou um e-mail errado ou achou algo suspeito

- Avise o canal de segurança responsável.
- Dispositivo suspeito: avise o time de segurança ou o suporte de TI.



No centro de tudo

Pessoas, básico e IA

Pessoas, o básico bem feito e a IA como aliada. Tudo o que vem antes depende disso.

- Pare, olhe e verifique
- 60 segundos
- O que proteger
- IA
- Cultura



Angela Rosso
Managing Director, Cybersecurity and AI at Accenture

Assistir ao vídeo

Pare, olhe e verifique

Um em cada três brasileiros já foi vítima de golpe virtual com perda financeira, segundo o Fórum Nacional de Segurança Pública. Com a IA, a saída é cultura e consciência: transformar o ser humano, visto por anos como o elo mais fraco, no elo mais forte.

Faça assim

Antes de clicar em um link, atender uma ligação ou passar informações, pare, olhe e verifique.



Daniel Peres
Cybersecurity Associate Director at Accenture

Assistir ao vídeo

60 segundos antes de agir

A maioria dos incidentes não acontece por falta de tecnologia, e sim por uma decisão tomada com pressa. Antes de clicar, aprovar uma transferência, compartilhar um documento ou instalar um aplicativo, vale parar para verificar.

Faça assim

Reserve 60 segundos antes de agir e transforme essa atenção em hábito diário.



Luiz Felipe
SOC OT Lead for Latin America at Accenture

Assistir ao vídeo

Saiba o que proteger

Há excelentes tecnologias para proteger o negócio, mas nem sempre sabemos o que de fato é relevante. Em incidentes, muitas vezes a máquina mais exposta era a que deveria ter a melhor proteção. Saber o que importa é governança.

Faça assim

Pergunte qual sistema é o mais importante para a empresa e comece a corrigir por ele.



Pedro Prudencio

Latam Cyber Defense and Resilience Lead, Managing Director at Accenture

Assistir ao vídeo

IA: defesa e ataque

A IA já falsifica rosto, voz e jeito de falar, e uma chamada de vídeo do chefe pedindo uma transferência pode ser falsa. Mas ela também protege, identificando ataques com mais velocidade. A tecnologia evolui dos dois lados.

Faça assim

Diante de um pedido urgente e fora do comum, mesmo de alguém conhecido, confirme por outro canal. Na era da IA, reconhecer não basta: é preciso verificar.



Thais Marella

HRPB for Accenture Cybersecurity LATAM

Assistir ao vídeo

Segurança também é cultura

A cultura de cibersegurança se constrói nas escolhas e nos comportamentos de cada dia. Com a IA e os agentes, é preciso preparar as pessoas, desenvolver competências e promover o uso responsável e seguro da tecnologia.

Faça assim

Integre a segurança à forma como você age, pensa e faz negócios. A mudança começa em cada um.



Sobre a Accenture

A Accenture é uma empresa de reinvenção de negócios e tecnologia. Nossa ambição é ser a parceira preferida de nossos clientes em suas jornadas de reinvenção. Queremos liderar a adoção segura e em larga escala de inteligência artificial e ser a empresa mais focada no cliente, habilitada por IA e um excelente lugar para trabalhar em todo o mundo.

Nossos 814 mil profissionais, aproximadamente, reúnem profundo conhecimento de diferentes setores e funções, com capacidades que abrangem estratégia, processos, modelos operacionais, gestão da mudança, talentos, dados, tecnologia e IA. Oferecemos essa expertise por meio de consultoria, serviços gerenciados, ativos e plataformas proprietárias e, cada vez mais, software.

Desenvolvemos inovações e novas soluções com base em nossa experiência em diferentes setores, o que nos permite aplicar insights relevantes, capacidades e práticas de referência de setores adjacentes para enfrentar novos desafios e aproveitar oportunidades emergentes de negócios. Atendemos mais de 9 mil clientes e geramos receitas de aproximadamente US$ 74 bilhões no ano fiscal de 2026. Visite-nos em **www.accenture.com.br**.

Siga nossas redes sociais

@accenturebrasil

Copyright © 2026 Accenture. Todos os direitos reservados.