

STATE OF DIGITAL TRUST

PILLARS OF TRUST

C-LEVEL, DIRECTOR
MANAGER INSIGHTS

DIGITAL TRUST READINESS
SCORE

1245.54°
753234.77°

IDENTITY

AUTOMATION

433.6°
24567.76°

ID 7021.4

THREATS

XX
SECURITY ALERT

ZERO TRUST

ENTERPRISES
EMPLOYEES
CUSTOMERS

6578.854°
6785.77°

GLOBAL STUDY

NOVEMBER 2022

digicert®



RELATÓRIO DA PESQUISA DE CONFIANÇA DIGITAL 2022

Estamos passando por uma rápida transição de um mundo de interações presenciais para um mundo conectado digitalmente e sempre ativo. A transformação digital é o motor dessa transição. E a pandemia também. Mas como estabelecer confiança nesse novo mundo?

Como podemos:

- Garantir que as pessoas (e os dispositivos) com os quais nos conectamos são legítimos?
- Saber se os dados que consumimos são seguros?
- Verificar se não estamos sujeitos a violações de segurança ou ataques de negação de serviço?
- Ter certeza de que os aplicativos e serviços que usamos não estão comprometidos?

Essa não é uma tarefa fácil. Este novo mundo expandiu a superfície dos ataques, e o custo dos lapsos de segurança explodiu. Quando se vai além dos custos legais, regulatórios e de remediação, o maior custo de todos pode ser a perda da fidelidade do cliente e os danos à marca. Um relatório Forbes Insights concluiu que quase metade (46%) de todas as organizações enfrentou danos à reputação e marca devido a uma violação de segurança de terceiros¹.

Com isso, a confiança digital passou a ocupar o primeiro plano. Segundo Jennifer Glenn, diretora de pesquisa do IDC, a confiança digital é a base da proteção do mundo conectado e necessária para as organizações que desejam garantir que seus clientes, funcionários e parceiros tenham a confiança de que interações e processos de negócios online sejam seguros.

Na essência, a confiança digital proporciona a liberdade de participar totalmente do mundo digital.

A DigiCert, o maior fornecedor global de confiança digital, permite que indivíduos e empresas interajam online sabendo que sua presença no mundo digital está protegida, entendendo melhor como as organizações globais percebem a confiança digital e o quão avançados seus esforços digitais estão.

A pesquisa Estado da confiança digital em 2022 da DigiCert investiga onde empresas, funcionários e consumidores de todo o mundo adotaram a confiança digital.

¹O impacto do risco de TI na reputação – Forbes Insights

O que é a confiança digital?

Segundo Jennifer Glenn, diretora de pesquisa do IDC, a confiança digital é a base da proteção do mundo conectado e necessária para as organizações que desejam garantir que seus clientes, funcionários e parceiros tenham a confiança de que interações e processos de negócios online sejam seguros.

A base da confiança digital é composta por quatro componentes essenciais:

1. Padrões que definem os requisitos de confiança para uma determinada tecnologia ou setor.
2. Conformidade e operações que geram ou verificam certificados digitais que estabelecem segurança (por meio de

identidade, integridade e criptografia), com a garantia de que atendem aos requisitos definidos pelos órgãos responsáveis pelos padrões.

3. Gerenciamento de confiança que garante que as empresas administrem com sucesso o ciclo de vida dos certificados e centralizem a visibilidade e o controle sobre seu uso.
4. Confiança conectada que estende a segurança por meio de cadeias de suprimento mais complexas (como ocorre com software, dispositivos e conteúdo).

A confiança digital se origina desses quatro componentes essenciais. As empresas podem depender de terceiros para algumas ou todas essas atividades, ou gerenciá-las internamente.

“A confiança digital é a base da proteção do mundo conectado.”

—Jennifer Glenn,
diretora de pesquisa, IDC



A CONFIANÇA DIGITAL IMPORTA

A necessidade de confiança digital ressoou com os entrevistados, pois 100% das empresas afirmam que a confiança digital é importante, e a maioria (90%) diz que é extremamente importante. É tão importante, na verdade, que quase dois terços mudaram de fornecedor após perderem a confiança nesse fornecedor. E praticamente todas as empresas (99%) acreditam que é possível que seus clientes mudem para um concorrente caso percam a confiança na empresa. Quase a metade (47%) acredita que esse resultado seria provável.

Funcionários de empresas também adotaram completamente a confiança digital: 100% deles dizem que ela é importante, e 86% afirmam que é extremamente importante. Em suas funções na empresa, 99% considerariam mudar de fornecedor caso perdessem a confiança, com cerca de metade (51%) afirmando que a mudança seria “provável”.

E, finalmente, dois terços (68%) dos consumidores dizem que a confiança digital é importante, com um terço (36%) afirmando que é extremamente importante. Na verdade, metade (47%) deixou de fazer negócios com uma empresa na qual deixou de confiar. Pensando no futuro, 84% considerariam mudar de fornecedor, e (57%) afirmam que a mudança seria provável. Vale destacar que, quanto mais ricos são os consumidores, mais afirmam que a confiança digital é importante (58% dos consumidores com renda acima da média dizem que a confiança digital é importante).

Metodologia

A empresa Eleven Research, de Dallas, realizou a pesquisa Estado da confiança digital (2022) em setembro de 2022. A pesquisa foi conduzida por telefone e e-mail, com 400 empresas e 400 consumidores em todo o mundo.

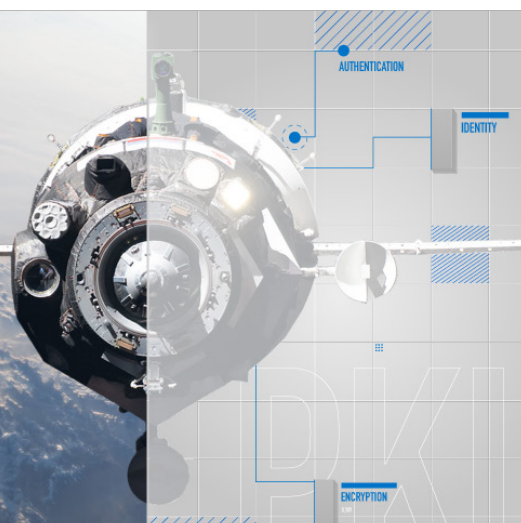
Empresas

Quatrocentos diretores e gerentes de nível sênior em TI, segurança de informações e DevOps em empresas com mais de 1.000 funcionários responderam à pesquisa. As respostas foram globais: Figura A (consulte p. 5)

Consumidores

Pesquisamos 400 consumidores globais (mesmas regiões) cobrindo uma grande variedade em faixa etária, gênero, orientação política e status econômico: Figura B (consulte p. 5)

“99% dos funcionários das empresas considerariam mudar de fornecedor se perdessem a confiança digital.”



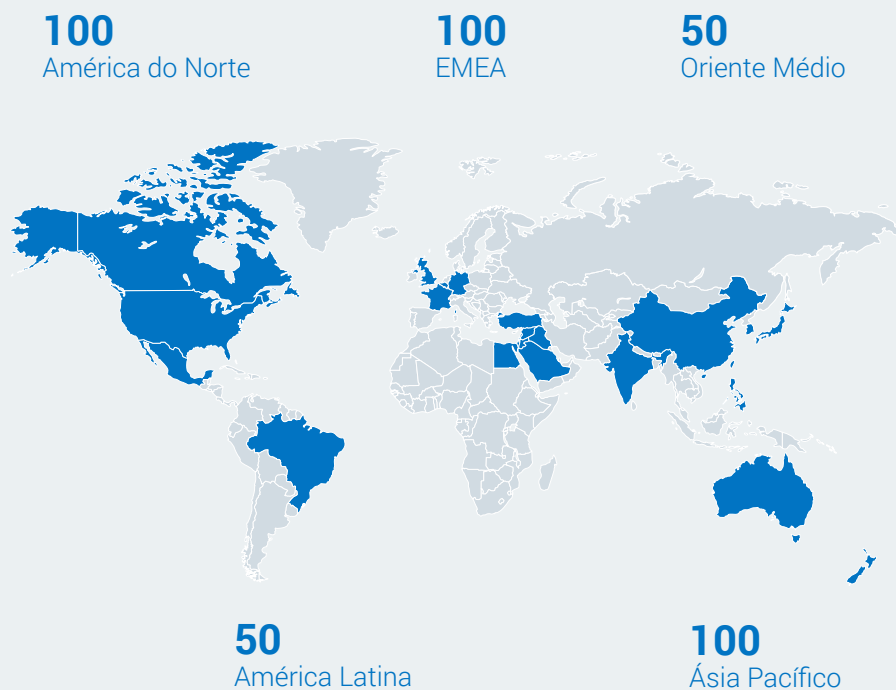


Figura A.

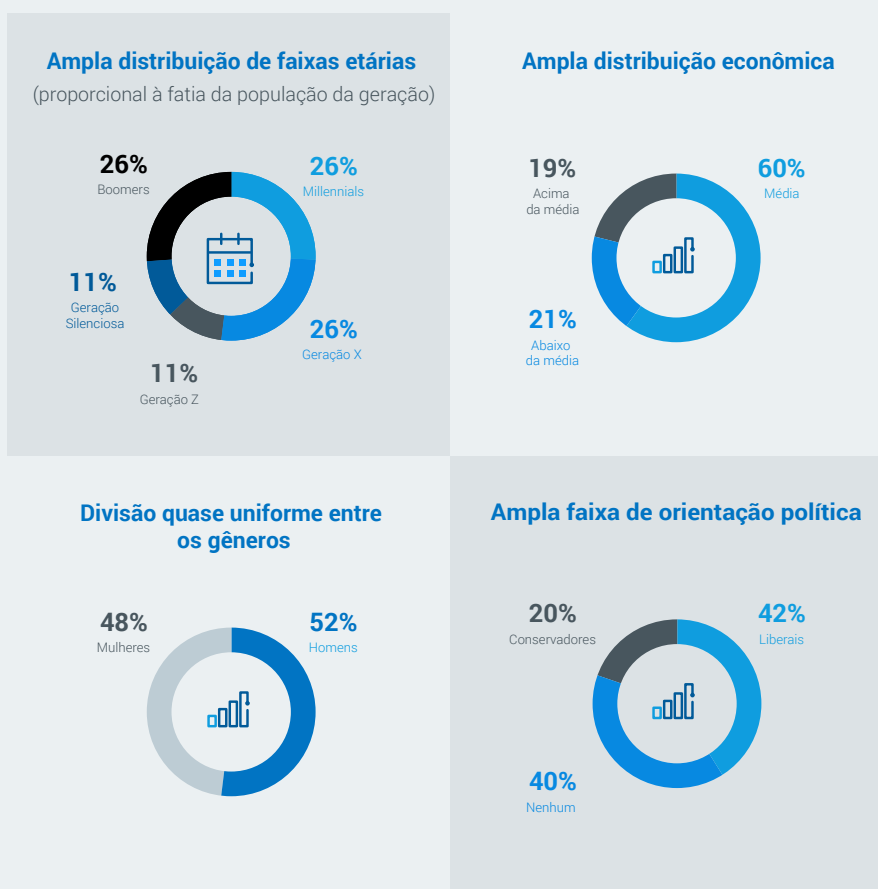
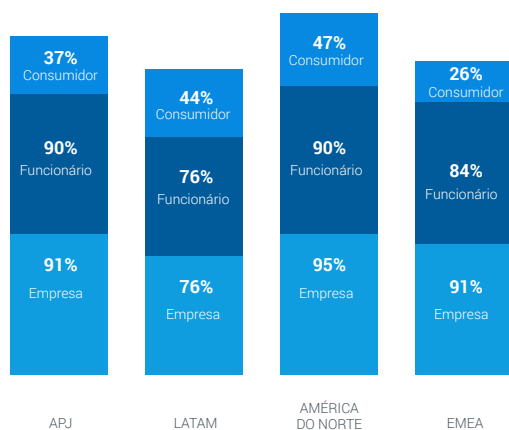


Figura B.

A IMPORTÂNCIA DA CONFIANÇA DIGITAL VARIA

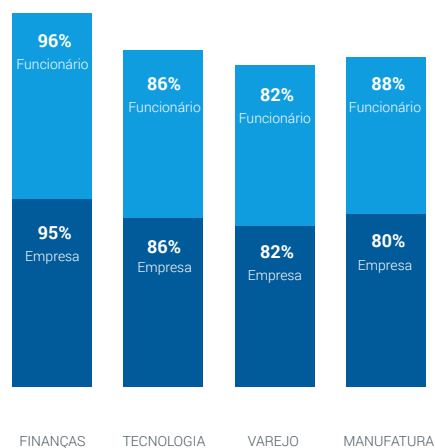
Empresas, funcionários e consumidores concordam que a confiança digital é importante, mas o grau de importância depende de vários atributos.

CONFIANÇA DIGITAL COMO EXTREMAMENTE IMPORTANTE POR REGIÃO



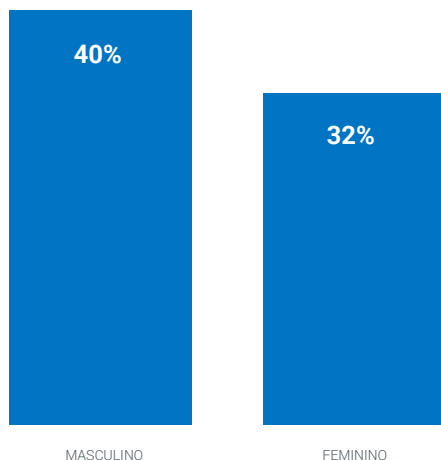
Em relação a empresas e funcionários, o atraso da América Latina em relação à confiança digital é muito importante. Em relação aos consumidores, as regiões APJ e EMEA ficam para trás. É uma surpresa que 26% dos consumidores da EMEA afirmem que a confiança digital é extremamente importante, considerando as rígidas leis de proteção de dados da UE promulgadas em 2018.

CONFIANÇA DIGITAL COMO EXTREMAMENTE IMPORTANTE POR SETOR



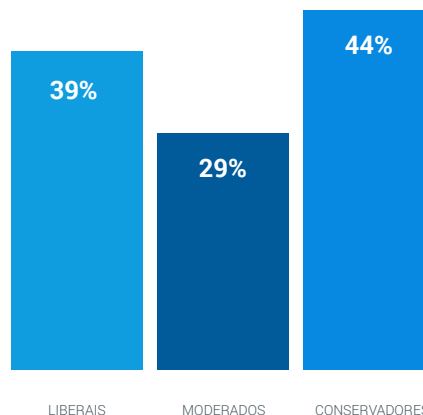
Como se pode esperar, empresas do setor financeiro têm maior probabilidade de dizer que a confiança digital é extremamente importante.

CONFIANÇA DIGITAL COMO EXTREMAMENTE IMPORTANTE POR GÊNERO (CONSUMIDORES)



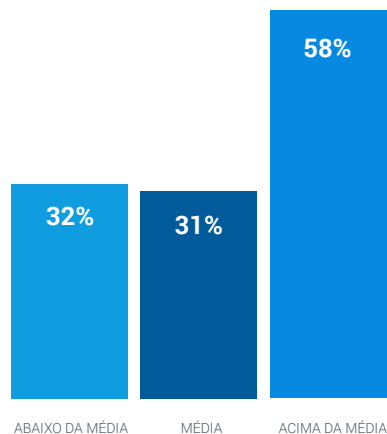
A confiança digital importa mais para consumidores do sexo masculino.

CONFIANÇA DIGITAL COMO EXTREMAMENTE IMPORTANTE POR AFILIAÇÃO POLÍTICA (CONSUMIDORES)



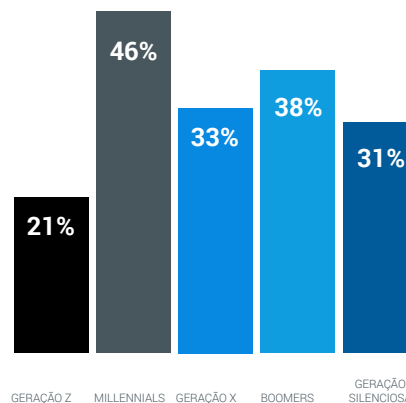
Finalmente liberais e conservadores podem concordar! Ambos têm maior probabilidade de dizer que a confiança digital é extremamente importante.

CONFIANÇA DIGITAL COMO EXTREMAMENTE IMPORTANTE POR RENDA (CONSUMIDORES)



Além disso, a confiança digital importa muito mais para consumidores com renda acima da média.

CONFIANÇA DIGITAL COMO EXTREMAMENTE IMPORTANTE POR GERAÇÃO (CONSUMIDORES)



É interessante observar que as duas gerações mais novas (e as únicas que são nativas digitais) têm a menor e a maior probabilidade de afirmar que a confiança digital é extremamente importante.

O QUE CAUSA O INTERESSE NA CONFIANÇA DIGITAL?

Existe um interesse universal na confiança digital. Mas qual é o motivo? O que estimula esse interesse? Encontramos diversos fatores.

Crescente importância dos dados. Segundo os entrevistados, esse é o principal motivo. Por quê? Porque os dados crescem a uma taxa composta de 23%². Explicando de outra forma, foram necessários 70 anos para que o mundo acumulasse 97 zettabytes de dados no fim de 2021. Até 2025, apenas quatro anos depois, esse número praticamente dobrará (174 ZB). Isso representa mais de 20.000 gigabytes para cada pessoa do mundo até 2025!

No entanto, não se trata apenas do volume dos dados; seu grau de importância também conta. Os dados contêm milhares de informações de identificação pessoal (PII), como o que compramos, os sites que visitamos, nossos prontuários médicos, redes sociais, fotos e muito mais.

Maior superfície de ameaças. A empresa transformou as relativamente estáticas redes de dados de data centers, escritórios e sites remotos em redes híbridas muito mais complexas. Essas novas redes conectam data centers, escritórios e sites remotos, ao mesmo tempo em que adicionam milhares de locais de trabalho remoto, nuvens, dispositivos digitais, redes de borda e dispositivos IoT.

Nessa nova rede sem limites definidos, existe uma escala muito maior de pontos de ataque.

Expectativas dos clientes. Como vimos na última seção, 100% das empresas e 68% dos consumidores avaliam a confiança digital como importante. Caso percam a confiança em um fornecedor, é provável que mudem para a concorrência. A confiança digital passou a ser um ativo que garante a própria existência.

Aumento do número de pessoas mal-intencionadas.

O número de pessoas mal-intencionadas cresce a cada ano. Elas incluem:

- Hackers "black hat"
- Cibercriminosos
- Ciberterroristas
- Hacktivistas
- Ameaças internas
- Hackers de estado-nação
- Trolls e caçadores de emoções

A prova do aumento do número de pessoas mal-intencionadas pode ser vista no número recorde de reclamações que o IC3 recebeu em 2021: 847.376 reclamações registradas, um aumento de 7% em relação a 2020³.



²Crescimento imenso previsto para big data - IDC

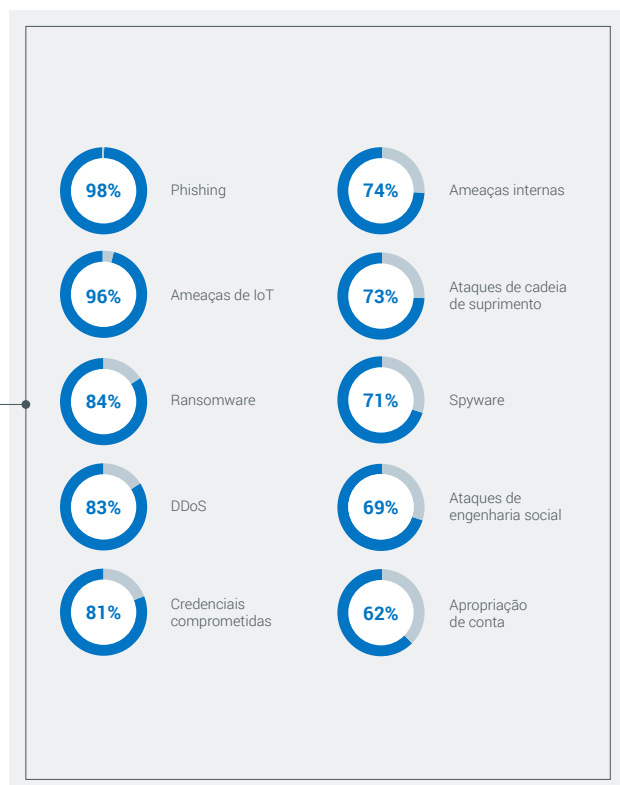
³FBI Internet Crime Complaint Center (IC3)

O QUE ESTÁ EM JOGO?

O que as empresas protegem? 100% dos entrevistados empresariais citam a fidelidade do cliente como um fator importante. Isso faz sentido quando se considera a possibilidade de que os clientes mudem para a concorrência caso percam a confiança em uma empresa.

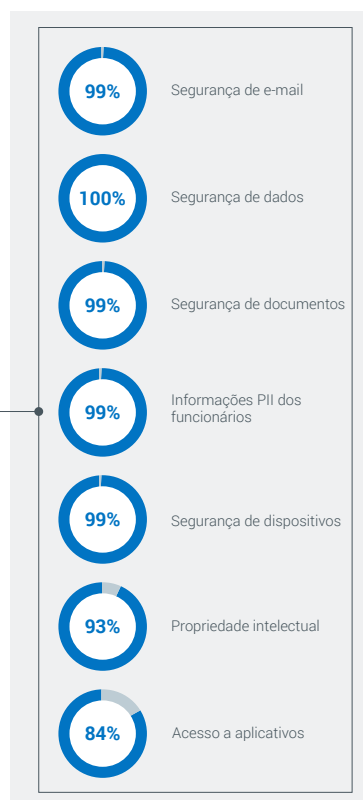
Os entrevistados listaram os seguintes tipos de ataques como os mais temidos (na ordem):

PARA EMPRESAS...



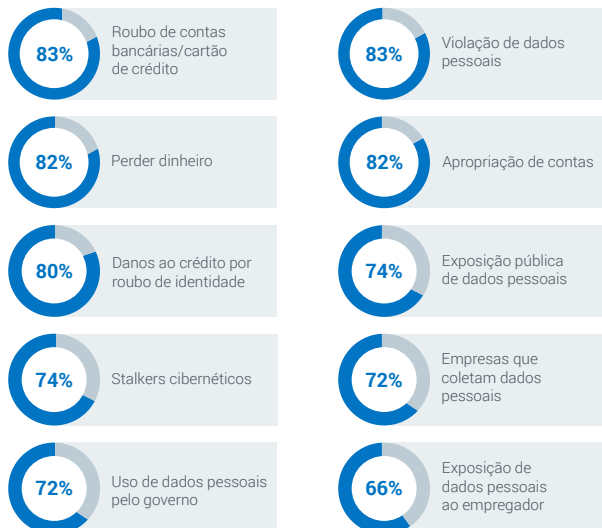
Os funcionários de empresas têm uma preocupação diferente suas informações pessoais.

PARA FUNCIONÁRIOS...

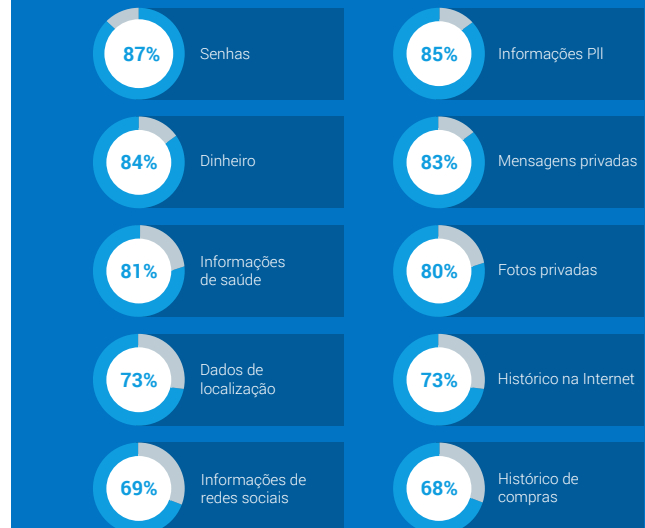


E, finalmente, os consumidores têm uma grande variedade de preocupações:

OS CONSUMIDORES TEMEM ESTES ATAQUES...



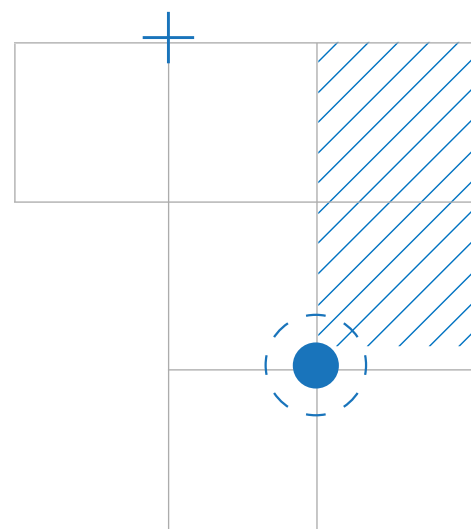
OS CONSUMIDORES QUEREM PROTEGER...



Queríamos saber se as empresas concordam com os consumidores sobre ajudar a proteger o que mais importa para eles (senhas, informações de identificação pessoal - PII, etc.). Praticamente todos os ataques que comprometem os dados dos consumidores começam com ataques por e-mail⁴. Apesar de tudo o que as empresas fazem para proteger os consumidores, elas classificaram a proteção contra ataques por phishing em penúltimo lugar quando se trata de seu próprio desempenho. Além disso, classificaram o phishing como o tipo de ataque que mais as preocupa.

Assim, embora as empresas se concentrem no que mais importa para os consumidores, elas estão longe de atingir o nível de segurança que os consumidores gostariam de ver.

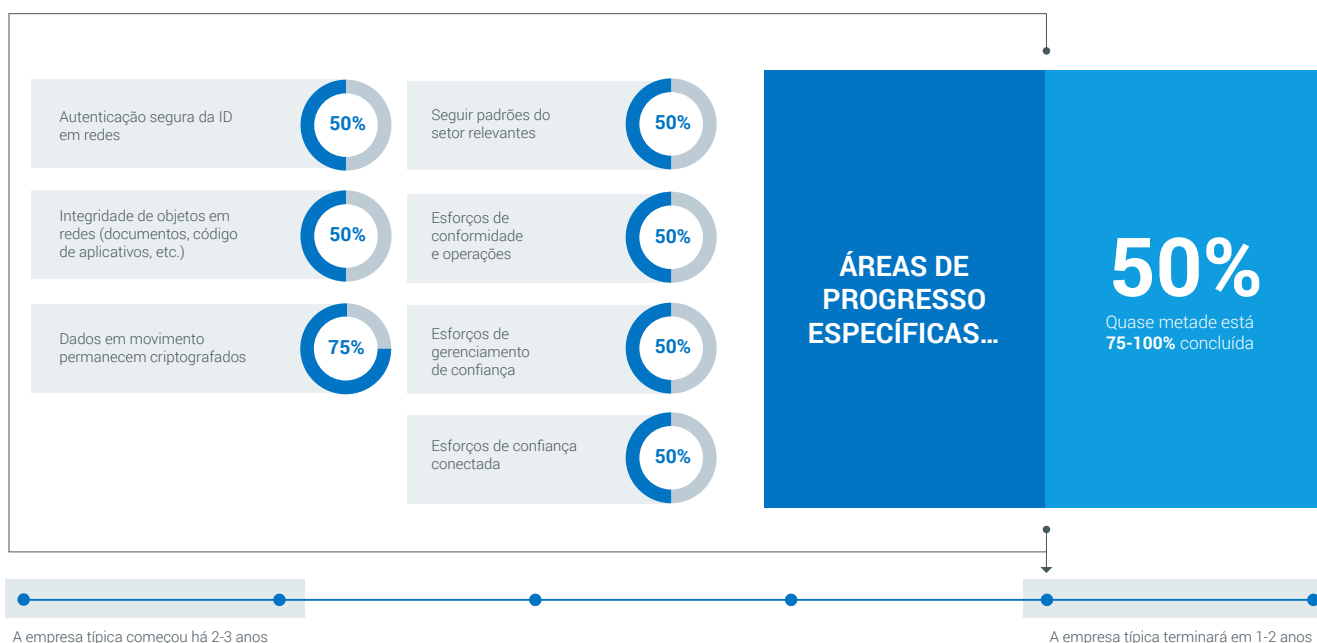
⁴Por que sua empresa precisa de segurança de e-mail aprimorada
- Guardian Digital



COMO AS EMPRESAS OTIMIZAM A CONFIANÇA DIGITAL?

As empresas estão envolvidas com a confiança digital. A organização típica começou a desenvolver a confiança digital há dois ou três anos e concluiu pelo menos 75% da jornada até agora. A jornada estará completa no próximo ano ou dois.

A confiança digital tem muitas facetas. Investigamos onde as empresas mais avançaram.



Metas de confiança digital: As empresas afirmaram claramente que a principal meta da confiança digital é a fidelidade do cliente. 100% avaliaram essa meta como a mais importante. No entanto, existem outras metas.



Desafios da confiança digital: As empresas estão bastante avançadas na jornada da confiança digital, mas isso não é fácil. O principal desafio citado pela TI foi o gerenciamento dos certificados digitais, classificado como importante por 100% das empresas. A conformidade regulatória e o tratamento de um imenso escopo de proteção ocupa um segundo lugar bastante próximo, com 99%. Completando esses desafios estão a complexidade (a proteção de uma rede dinâmica e complexa com vários fornecedores) e a ausência de especialização da equipe.

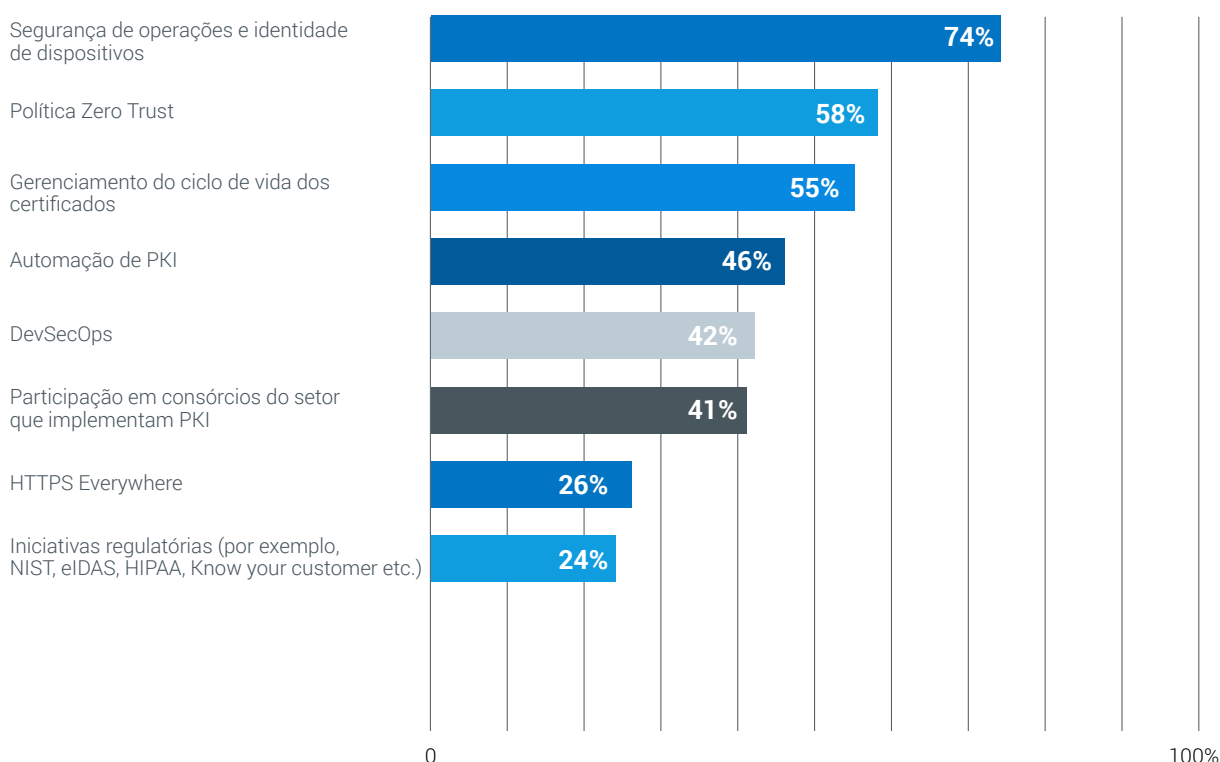


Práticas de confiança digital: Uma grande variedade de iniciativas pode afetar a confiança digital de uma empresa. A maioria das empresas está pelo menos um pouco envolvida nessas iniciativas, mas é útil ver quais iniciativas as empresas já implementaram completamente.

Em primeiro lugar está a segurança de operações e identidade de dispositivos, totalmente implementada por 74% das empresas. Em seguida estão as políticas de confiança zero (Zero Trust), mas elas só foram totalmente implementadas por 58% das empresas. A única outra iniciativa implementada por mais da metade das empresas (55%) é o gerenciamento do ciclo de vida dos certificados. Finalizando a lista estão:

Q22: Qual é seu envolvimento com as seguintes práticas de confiança digital?

Já implementada



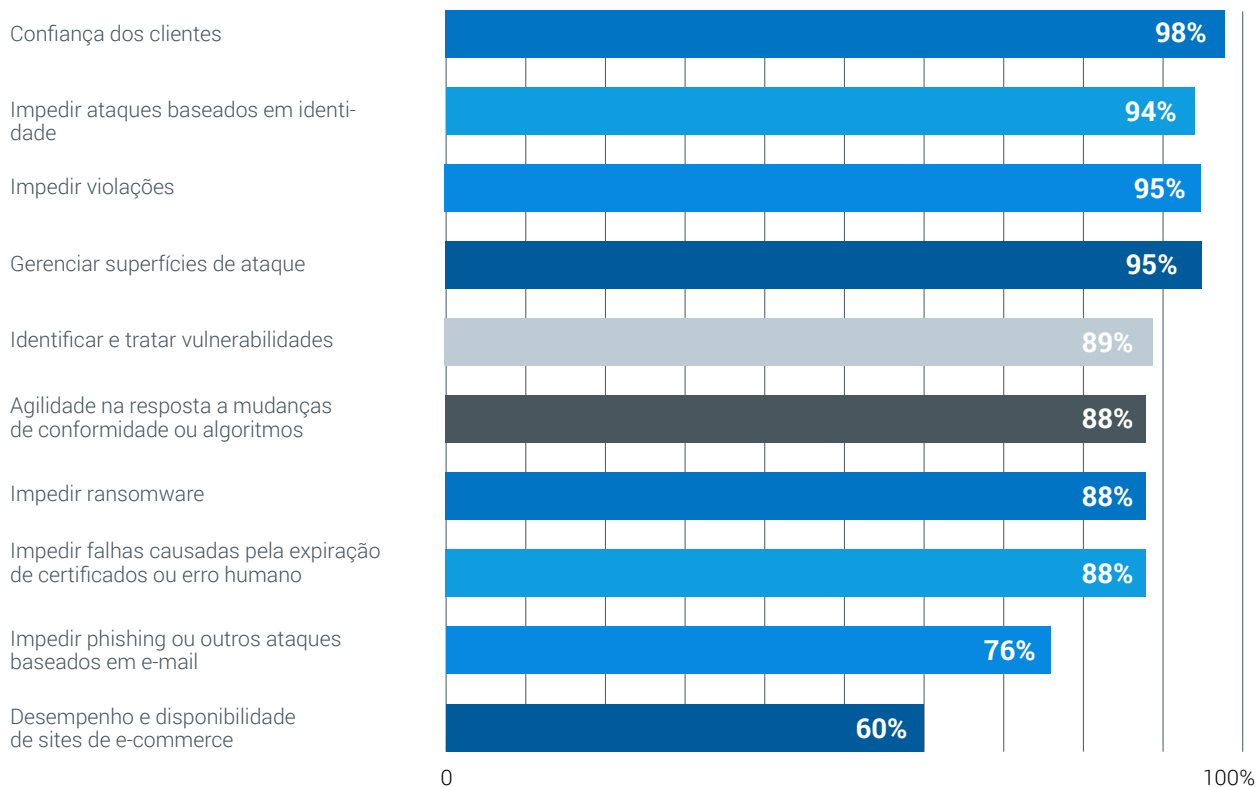
QUAIS OS RESULTADOS DAS EMPRESAS QUANTO A MÉTRICAS DE CONFIANÇA DIGITAL?

Em relação a um vasto conjunto de metas de confiança digital, o desempenho das empresas é bastante satisfatório. Por exemplo, considere a confiança do cliente, a meta principal das empresas. 98% têm ótimo desempenho nessa meta, e 61% têm desempenho muito bom. O desempenho das empresas também é ótimo quando se trata de evitar violações (95%, dos quais 51% têm excelente desempenho) e ataques baseados em identidade (94%, com 50% delas apresentando excelente desempenho).

Na verdade, para oito das dez métricas estudadas, pelo menos sete de oito empresas afirmaram que estavam se saindo bem. O desempenho menos satisfatório relaciona-se ao combate ao phishing ou outros ataques baseados em e-mail e no desempenho e disponibilidade de sites de e-commerce (76% e 60%, respectivamente).

Q23: Como você avalia seu desempenho em cada uma das seguintes métricas de confiança digital?

Um pouco/extremamente bem



Os clientes estão vendo melhorias

Todas as empresas (100%) relatam que a confiança digital é importante para seus clientes, com 91% afirmando que seus clientes classificam a confiança digital como extremamente importante.

Por isso, é essencial compreender como os clientes percebem a confiança digital. Da perspectiva das empresas, essa é uma boa notícia, com 99% das empresas afirmando que os clientes confiam mais em suas práticas hoje do que no passado. Quase três quartos (73%) afirmam que a confiança é significativamente maior.

O que as empresas pensam a respeito? Elas compartilham desse otimismo? Na verdade, os números são quase idênticos. Quando solicitadas a avaliar a confiança nas empresas com as quais interagem, 98% afirmam que ela é maior hoje, e 76% afirmam que é muito maior.

Mas isso se relaciona a interações B2B. E o cenário B2C? Os números não são tão otimistas. Menos da metade afirma que sua confiança digital nas organizações com que lidam é maior hoje, e 54% afirmam que existe espaço para melhorias.

“91% dos clientes classificam a confiança digital como extremamente importante.”



Resultados da América do Norte

A América do Norte (Estados Unidos e Canadá) lidera o mundo quando se trata de classificar a confiança digital como extremamente importante. Isso é verdade para empresas, funcionários e consumidores.

Os consumidores da América do Norte são os mais preocupados com ameaças cibernéticas (como acesso indevido a contas bancárias ou cartões de crédito e roubo de dinheiro) do que os consumidores de qualquer outro lugar do mundo, à exceção do Pacífico Asiático (APAC). (91% dos consumidores da APAC preocupam-se com essas ameaças, contra 85% dos consumidores

da América do Norte e 77% e 78% de EMEA e LATAM, respectivamente.)

Tudo isso mostra a alta pontuação que os consumidores concedem às empresas da América do Norte. Em relação ao sucesso da confiança digital, 31% dos consumidores da América do Norte afirmam que têm significativamente mais confiança nas empresas com as quais fazem negócios. Os consumidores da APAC estão no meio do caminho, com 19%. Isso se compara a 24% para consumidores da América Latina, e apenas 19% e 15% para consumidores da APAC e EMEA, respectivamente.

Resultados da APAC

De forma global, a região APAC vê a confiança digital como extremamente importante. Ela dá mais importância à confiança digital do que qualquer outra região, exceto a América do Norte.

Em parte, isso ocorre porque os consumidores da APAC são os mais preocupados com ameaças cibernéticas (como acesso indevido a contas bancárias ou cartões de crédito e roubo de dinheiro) do que os consumidores de qualquer outro lugar do mundo. (91% dos consumidores da APAC preocupam-se com essas ameaças, contra

85% dos consumidores da América do Norte e 77% e 78% de EMEA e LATAM, respectivamente.)

Em relação ao sucesso da confiança digital, os consumidores da APAC estão no meio do caminho, com 19% afirmando que têm significativamente mais confiança nas empresas com as quais fazem negócios. Os consumidores da América do Norte e da América Latina relatam 31% e 24%, respectivamente, enquanto os consumidores da EMEA relatam apenas 15%.

Resultados da LATAM

A América Latina está atrás do resto do mundo quando se trata de ver a confiança digital como extremamente importante.

Isso ocorre em parte porque os consumidores da América Latina estão menos preocupados com ameaças cibernéticas (como acesso indevido a contas bancárias ou cartões de crédito e roubo de dinheiro) do que a maioria dos consumidores. (Apenas 78% dos consumidores da LATAM preocupam-se com essas ameaças, contra 91% dos consumidores da APAC, 85% dos

consumidores da América do Norte e 77% dos consumidores da EMEA.)

Em relação à confiança digital, os consumidores da LATAM relatam sucesso relativamente alto, com 24% dos consumidores da LATAM afirmando que têm significativamente mais confiança nas empresas com as quais fazem negócios. Em comparação, os consumidores da América do Norte relatam 31%, enquanto os consumidores da APAC e da EMEA relatam 19% e 15%, respectivamente.

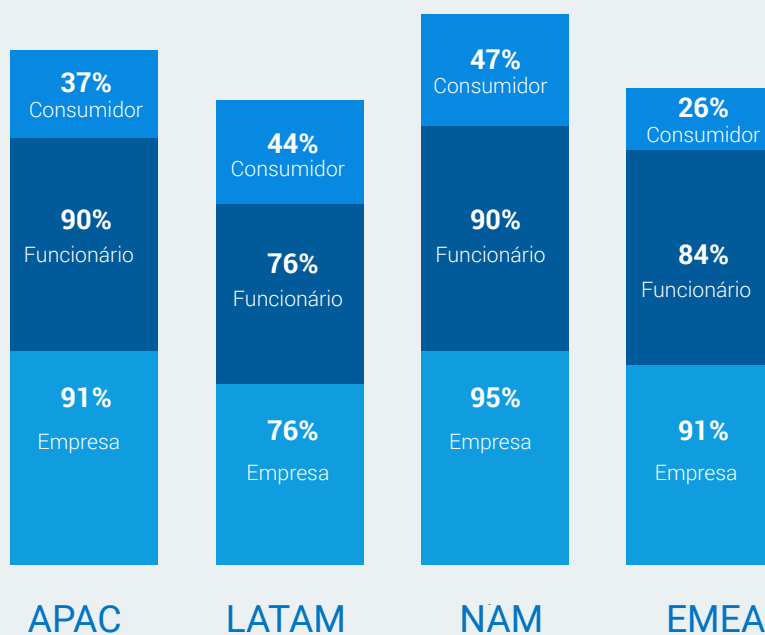
Resultados da EMEA

Para uma região com uma das leis de proteção de dados (LGPD) mais rígidas, os consumidores da EMEA têm uma atitude surpreendentemente indiferente quando se trata de confiança digital. De forma geral, a EMEA está em terceiro lugar na avaliação da importância da confiança digital. No entanto, uma investigação dos dados mostra que as empresas da EMEA têm um grande interesse, e os funcionários têm um interesse médio na confiança digital. É no nível do consumidor que vemos que os números relacionados à importância da confiança digital é quase metade dos números da América do Norte.

Isso está ligado à preocupação com ameaças cibernéticas. Os consumidores da EMEA têm o nível mais baixo de preocupação com ameaças cibernéticas, como acesso indevido a contas bancárias e cartões de crédito ou roubo de dinheiro. Apenas 77% dos consumidores da EMEA preocupam-se com essas ameaças, em comparação a 78% dos consumidores da LATAM, 85% dos consumidores da América do Norte e 91% dos consumidores da APAC.

Isso se relaciona com a porcentagem relativamente baixa de consumidores da EMEA que dizem que sua confiança nas empresas com as quais fazem negócios aumentou nos últimos anos (apenas 15%). Isso está atrás da APAC (19%), LATAM (24%) e América do Norte (31%).

CONFIANÇA DIGITAL COMO EXTREMAMENTE IMPORTANTE POR REGIÃO



LIÇÕES DOS CONHECEDORES DA CONFIANÇA DIGITAL

Como vimos na última seção, as empresas parecem estar indo bastante bem em seus esforços de confiança digital. Queríamos saber se essa é uma verdade universal ou se algumas empresas se saíram consideravelmente melhor ou pior do que a média.

Para investigar o assunto, pontuamos as respostas das seguintes perguntas sobre métricas:

Guia de pontuação

- | | |
|--------------------|----|
| • Extremamente mal | -2 |
| • Um pouco mal | -1 |
| • Nem bem nem mal | 0 |
| • Um pouco bem | +1 |
| • Extremamente bem | +2 |

Em seguida, adicionamos três pontuações individuais para criar uma pontuação total para cada entrevistado. Dividimos os entrevistados em três níveis:

Níveis de confiança digital das empresas

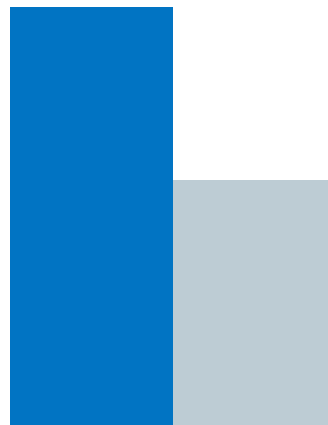
- Nível superior (pontuações no terço superior de todos os entrevistados)
- Nível médio (terço médio)
- Nível inferior (terço inferior)

Esses níveis mostram diferenças drásticas entre as melhores empresas (o nível superior) e as piores (o nível inferior).

Quanto melhor?

É evidente que o nível superior tem melhor desempenho com as métricas de confiança digital, já que é assim que dividimos os entrevistados em níveis. No entanto, é interessante observar o quanto o nível superior tem melhor desempenho do que o inferior. Por exemplo, três vezes mais empresas de nível superior relatam um bom desempenho e disponibilidade de sites de e-commerce, e 2,9 vezes mais empresas afirmam que se saem bem ao impedir ataques de phishing ou outros ataques baseados em e-mail. O nível superior vai de 10% melhor a 300% melhor em cada métrica:

1,7x



OS CLIENTES DE ORGANIZAÇÕES DO **NÍVEL SUPERIOR** TÊM SIGNIFICATIVAMENTE MAIS PROBABILIDADE DE CONFIAR NELAS DO QUE OS CLIENTES DO **NÍVEL INFERIOR**.

²Crescimento imenso previsto para big data - IDC

³FBI Internet Crime Complaint Center (IC3)

AS MELHORES EMPRESAS ESTÃO SE SAINDO **MUITO** MELHOR COM A CONFIANÇA DIGITAL



Por que o nível superior se sai tão melhor?

Existe uma variedade de diferenças marcantes entre o nível superior e o nível inferior que justifica as maiores diferenças entre os resultados de confiança digital:

- **Atitudes:** O nível superior tem quatro vezes e meia mais probabilidade de acreditar que a perda da confiança do cliente levará à perda desse cliente. Ele também tem mais probabilidade de acreditar que a confiança digital afeta sua marca, vendas e margem. Além disso, tem 5,6 vezes mais probabilidade de afirmar que mudaria de parceiro caso perdesse a confiança nesse parceiro.
- **O primeiro passo:** O nível superior está mais além em sua jornada da confiança digital e completará essa jornada muito antes do nível inferior.
- **Mais preocupação com ameaças cibernéticas:** O nível superior leva as ameaças cibernéticas muito mais a sério. O nível superior tem 1,5 a 2,3 mais probabilidade de se preocupar com ameaças cibernéticas.
- **Mais engajamento com proteções cibernéticas comuns:** O nível superior tem até três vezes mais probabilidade de se engajar em proteções de segurança cibernética.

MAIS PROBABILIDADE DE QUE O
NÍVEL SUPERIOR SE ENGAJE EM:

Participação na implementação da PKI



Política Zero Trust



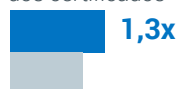
Automação de PKI



HTTPS Everywhere



Gerenciamento do ciclo de vida dos certificados

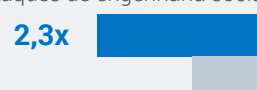


Segurança de operações e identidade de dispositivos



O **NÍVEL SUPERIOR** ESTÁ MAIS
PREOCUPADO COM ALGUMAS AMEAÇAS
CIBERNÉTICAS IMPORTANTES:

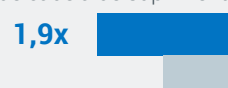
Ataques de engenharia social



Spyware



Ataques de cadeia de suprimento



Apropriação de conta



Ransomware



Onde a confiança digital deve residir?

Decidir onde posicionar a confiança digital em uma organização empresarial é importante. Existe uma clara divergência de opinião entre as empresas do nível superior e do nível inferior.

Em sua esmagadora maioria, o nível superior afirma que o CIO deve administrar a confiança digital na organização de TI, enquanto o nível inferior acredita que isso deve ficar a cargo das operações de segurança.

Isso não significa desconsiderar as operações de segurança ou sua função, que são vitais para uma organização. Essa conclusão confirma a visibilidade para o CIO da presença mais ampla da tecnologia em uma organização e da importância da confiança digital para o sucesso de uma organização orientada por tecnologia. Esse resultado reflete a abordagem estratégica das empresas do nível superior à confiança digital.

VISÃO DA DIGICERT

A DigiCert, o maior fornecedor global de confiança digital, está envolvida na confiança digital desde o início, permitindo que indivíduos e empresas interajam online sabendo que sua presença no mundo digital está protegida. Nossa recomendação para as empresas que desejam replicar o sucesso demonstrado pelos “Conhecedores da confiança digital” do nível superior é considerar seguir estes cinco procedimentos:



Torne a confiança digital um imperativo estratégico. Esse foi um dos principais diferenciadores para as empresas do nível superior, que reconheceram que a confiança digital afeta resultados importantes, como marca, fidelidade do cliente, receita e margens.



Estabeleça um departamento de confiança digital na função de tecnologia de sua organização, com um líder explícito que tenha poder de decisão.



Reconheça que a conscientização sobre a confiança digital está aumentando entre seus usuários, incluindo consumidores, e que seu sucesso nos negócios e sua reputação estão vinculados diretamente à sua capacidade de garantir a confiança digital de forma mais avançada.

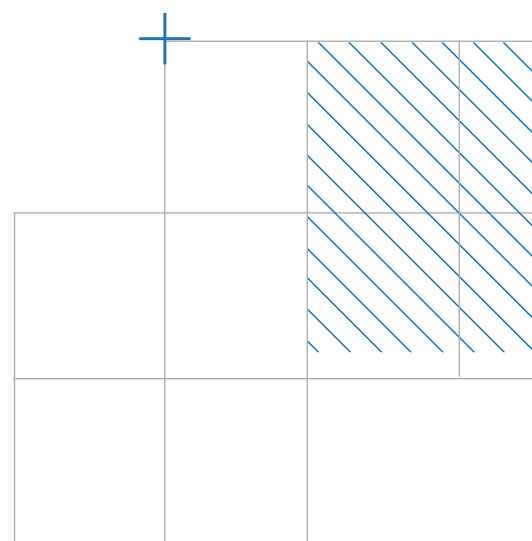


Contrate ajuda especializada em sua busca pela confiança digital. Um dos desafios da confiança digital citados pelas empresas é a ausência de especialização da equipe. Certifique-se de que seus parceiros tenham um portfólio abrangente, com os componentes essenciais da confiança digital, e que possam fornecer soluções para o gerenciamento da confiança unificada para toda a sua organização.



Lembre-se: seus clientes se importam com a confiança digital. Defina canais de comunicação de confiança digital claros com os clientes, explicando não só seu compromisso com a confiança digital mas também seu progresso.

Essa atitude está alinhada com um conhecido estudo da Bain & Company⁵, que concluiu que aumentar a taxa de retenção de clientes em 5% aumenta os lucros em 25% a 95%. Considerando a probabilidade de que os clientes deixem uma empresa caso percam a confiança nela, maximizar a confiança digital deve ser uma atividade obrigatória.



⁵Recomendações para reduzir custos – Bain & Company

|||



1245.54°
753234.72°

|||



IoT



digicert®