IBM **Security**

# X-Force Threat Intelligence Index 2022: Resumo executivo

IBM

# Índice

# Resumo executivo

O mundo continua a enfrentar uma longa pandemia, as mudanças de trabalho remoto e de retorno ao escritório e os novos cenários geopolíticos geram um sentimento de incerteza constante. Tudo isso resulta em caos, e é no caos que os criminosos cibernéticos atuam. Em 2021, a IBM Security® X-Force® identificou como os agentes de ameaça aproveitavam essa mudança de cenário para adotar táticas e técnicas a fim de se infiltrarem em organizações em todo o mundo.

O IBM Security X-Force Threat Intelligence Index mapeia as novas tendências e os padrões de ataque que observamos e analisamos a partir de nossos dados, considerando bilhões de pontos de dados que consistem em redes e dispositivos de detecção em terminais, resposta a incidentes (IR), rastreamento de nome de domínio, entre outros. Este relatório apresenta uma pesquisa baseada em dados coletados de janeiro a dezembro de 2021.

Oferecemos esses resultados como um recurso para os clientes IBM, pesquisadores do setor de segurança, criadores de políticas, veículos de comunicação e para a comunidade de profissionais de segurança e líderes de negócios como um todo.

Dado o cenário volátil e a evolução dos tipos e vetores de ameaças, nunca foi tão necessário adotar insights de inteligência contra ameaças para prevenir-se dos ataques e fortalecer seus assets mais críticos.

# Destaques do relatório

**Principal tipo de ataque:** o ransomware novamente destacou-se como principal tipo de ataque em 2021, embora a porcentagem de ataques remediados pela X-Force provenientes de ransomware foi reduzida em quase 9% ao longo dos últimos anos. REvil, um tipo de ransomware que a X-Force também chama de Sodinokibi, foi a cepa de ransomware mais comum observada pela X-Force pelo segundo ano consecutivo, representando 37% de todos os ataques de ransomware, seguido pelo Ryuk, com 13%. A atividade de aplicação da legislação provavelmente tem sido a maior força na redução de ataques de ransomware e de botnet de IoT em 2021, mas isso não impede uma possível recorrência em 2022.

**Vulnerabilidades da cadeia de fornecimento:** a segurança da cadeia de fornecimento foi colocada em primeiro plano por governos e criadores de políticas, com a ordem do executivo do governo Biden sobre segurança cibernética e a orientação do Departamento de segurança Interna dos EUA, CISA e NIST, reforçando a estratégia de zero trust. Essas diretrizes dão destaque às vulnerabilidades e aos relacionamentos confiáveis. A exploração da vulnerabilidade foi o principal vetor de ataque inicial no setor de manufatura, que sofria com os efeitos das pressões e atrasos da cadeia de fornecimento.

**Marcas que sofreram mais phishing:** a X-Force acompanhou de perto como os cibercriminosos usam kits de phishing ao longo de 2021, e nossa pesquisa revelou que a Microsoft, a Apple e a Google foram as três marcas que os criminosos mais tentaram imitar. Essas marcas foram usadas repetidamente em kits de phishing, com ataques provavelmente visando capitalizar sobre a popularidade e a confiança que os consumidores conferem a elas.

**Principais grupos ameaça:** o agente de ameaças suspeito do estado-nação iraniano ITG17 (MuddyWater), o grupo cibercriminoso (Trickbot) e o Hive0109 (LemonDuck) foram alguns dos grupos de maior atuação de ameaças observados pelos analistas de inteligência da X-Force em 2021. Grupos de ameaças do mundo inteiro tinham o objetivo de aprimorar seus métodos e se infiltrar em mais organizações. O malware usado era criado com técnicas de evasão de defesa mais avançadas, em alguns casos hospedado em sistemas de mensagens e plataformas de armazenamento baseados na nuvem para burlar os controles de segurança. Essas plataformas eram violadas para ocultar comunicações de controle e comandos no tráfego de rede legítimo. Os agentes de ameaças também continuaram a desenvolver versões de malware para Linux, para possibilitar sua transferência para ambientes de nuvem com mais facilidade.

# Principais estatísticas

## 21%

**Ataques de ransomware**

O ransomware foi o tipo de ataque mais observado pela X-Force no ano passado, caindo de 23% dos ataques no ano anterior para 21%. Os agentes de ransomware REvil (também conhecido como Sodinokibi) foram responsáveis por 37% de todos os ataques de ransomware.

## 17 meses

**Tempo médio até que uma gangue de ransomware mude de nome ou seja desativada**

As gangues de ransomware estudadas pela X-Force tiveram um tempo de vida médio de 17 meses antes de mudarem de nome ou serem desmembradas. REvil, uma das gangues mais bem-sucedidas, foi desativada em outubro de 2021 após 31 meses de atividades (dois anos e meio).

## 41%

**Porcentagem de ataques que usam phishing como acesso inicial**

As operações de phishing surgiram como o principal caminho para ataques em 2021, com 41% dos incidentes realizados por meio dessa técnica de acesso inicial remediados pela X-Force.

## 33%

**Aumento no número de incidentes causados por explorações de vulnerabilidade de 2020 a 2021**

Das cinco principais vulnerabilidades exploradas em 2021, quatro foram vulnerabilidades novas, incluindo a vulnerabilidade Log4j CVE-2021-44228, que foi classificada em segundo lugar, apesar de só ter sido divulgada em dezembro.

## 3 vezes mais

**Eficácia de cliques para campanhas de phishing direcionadas que incluem ligações telefônicas**

A taxa de cliques para a campanha de phishing direcionada média foi de 17,8%, mas as campanhas de phishing direcionadas que incluíram ligações telefônicas (vishing ou phishing por voz) foram três vezes mais eficazes, obtendo um clique de 53,2% das vítimas.

# 146%

**Aumento do ransomware para Linux com novo código**

A porcentagem de ransomware para Linux com código exclusivo (novo) aumentou 146% em relação ao ano anterior, de acordo com a Intezer, indicando um aumento no nível de inovação do ransomware para Linux.

# Nº1

**Classificação de ataques para o setor de manufatura**

O setor de manufatura substituiu os serviços financeiros como principal alvo de ataques em 2021, representando 23,2% dos ataques remediados pela X-Force no ano passado. O ransomware foi o principal tipo de ataque, somando 23% dos ataques a empresas de manufatura.

# 61%

**Porcentagem de violações do setor de manufatura em organizações ligadas a OT**

O setor de manufatura sofreu 61% dos incidentes em organizações ligadas a OT no ano passado. Além disso, 36% dos ataques a organizações ligadas a OT foram realizados com ransomware.

# 2.204%

**Aumento no reconhecimento relacionado a OT**

Os invasores aumentaram em 2.204% o reconhecimento de dispositivos de OT SCADA Modbus que podem ser acessados pela internet entre janeiro e setembro de 2021.

# 74%

**Ataques de IoT provenientes do botnet Mozi**

Em 2021, os ataques contra dispositivos IoT eram realizados pelo botnet Mozi 74% das vezes.

# 26%

**Parcela de ataques globais que atingiram a Ásia**

De todos os ataques, 26% tinham alvos na Ásia. A Ásia foi a região mais atacada de 2021.

# Recomendações para mitigação de risco

As ameaças que apresentamos neste relatório têm o potencial de causar preocupação, pois ressaltamos a grave e crescente ameaça de ransomware, novos modelos de ataques de BEC e phishing e destacamos várias explorações de dia zero que os agentes de ameaças realizaram no ano passado. No entanto, nossa intenção é que estas informações ajudem as empresas a se prepararem entendendo melhor o cenário atual de ameaças e a terem mais confiança ao tomar as ações necessárias para combater essas ameaças.

Alguns dos princípios de segurança que a X-Force considerou úteis no combate às ameaças atuais incluem a abordagem de zero trust, a automação de resposta a incidentes e recursos estendidos de detecção e resposta.

## Zero trust auxilia na redução de risco dos principais ataques

A abordagem zero trust é uma mudança de paradigma, uma nova maneira de entender os problemas de segurança, que supõe que uma violação já aconteceu e tem como objetivo aumentar a dificuldade para a invasão de uma rede. Em sua essência, significa entender onde os dados críticos residem e quem pode acessar esses dados, e criar medidas de verificação robustas em toda a rede para garantir que apenas as pessoas certas estejam acessando esses dados da maneira certa.

As pesquisas realizadas por especialistas de ameaças da X-Force confirmam que os princípios relacionados a uma abordagem de zero trust, para incluir a implementação de MFA e o princípio de privilégio mínimo, podem diminuir a suscetibilidade das organizações aos principais tipos de ataque identificados neste relatório, especialmente ransomware e BEC.

A aplicação do princípio de privilégio mínimo especialmente para controladores de domínio e contas de administradores de domínio pode aumentar as barreiras para os agentes de ransomware, pois muitos desses agentes procuram implementar o ransomware em uma rede a partir de um controlador de domínio comprometido. Além disso, a implementação da MFA aumenta a dificuldade para os cibercriminosos que tentam invadir contas de e-mail, exigindo que eles forneçam mais autenticação, além das credenciais roubadas.

Saiba mais sobre como criar uma abordagem zero trust →

# A automação da segurança aprimora a resposta a incidentes

A equipe de resposta a incidentes da X-Force atende a centenas de incidentes todo ano, em diversas regiões, auxiliando analistas internos de resposta a incidentes e solucionando diversos tipos de ataque. A velocidade é essencial, quer isso signifique identificar e eliminar agentes de ameaça antes que eles implementem o ransomware em uma rede ou resolver os problemas de forma rápida e eficiente para evitar o próximo incidente. Neste ambiente veloz, a automação da segurança é fundamental, ao delegar para máquinas as tarefas que podem exigir horas de um analista ou de uma equipe, e identificar mecanismos para melhorar os fluxos de trabalho.

Em meados de 2021, a IBM doou uma ferramenta de automatização de caça à ameaças para a Open Cybersecurity Alliance, visando auxiliar os analistas do centro de operações de segurança (SOC) a conduzir investigações forenses rápidas e lidar com incidentes cibernéticos. Além disso, a equipe de IR do X-Force usa o IBM Security QRadar SOAR para aprimorar suas capacidades de resposta a incidentes.

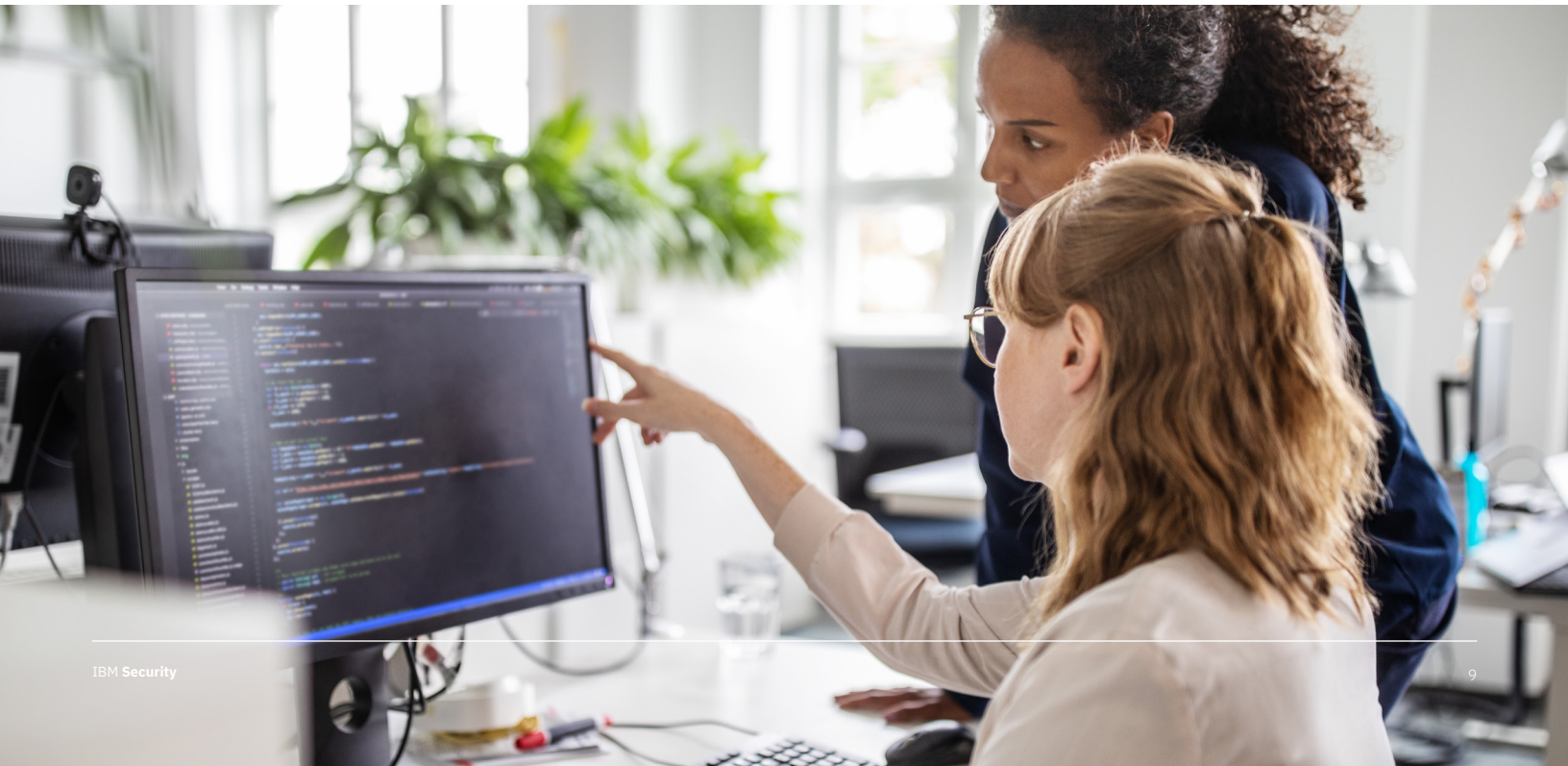
Saiba mais sobre os serviços de resposta a incidentes da IBM →

# Detecção e resposta estendidas proporcionam uma vantagem significativa sobre os invasores

As tecnologias de detecção e resposta, principalmente quando várias soluções diferentes são combinadas em uma solução estendida de detecção e resposta (XDR), oferecem às organizações uma vantagem significativa em identificação e erradicação de invasores de uma rede antes que eles consigam atingir o estágio final do ataque, como a implementação de ransomware ou o roubo de dados.

Em diversos casos, quando a equipe de IR da X-Force implementou um endpoint de detecção e resposta (EDR) ou uma solução XDR na rede de um cliente, a IR gerou imediatamente insights adicionais que ajudaram a identificar atividades de invasores e as solucionou rapidamente. As tecnologias XDR provavelmente estão ajudando a impulsionar o aumento no acesso ao servidor e outros tipos de ataque observados pela X-Force que indicam se um invasor foi identificado e barrado antes que a operação pudesse ser concluída.

Saiba mais sobre o IBM Security QRadar XDR →



# Recomendações

As recomendações a seguir incluem ações específicas que as organizações podem tomar para proteger suas redes contra as ameaças apresentadas neste relatório.

**Desenvolva um plano de resposta para ransomware.** Todos os setores e regiões estão suscetíveis a ataques de ransomware e a forma como sua equipe responde no momento crítico que sua equipe pode fazer toda a diferença quanto ao tempo e o capital perdido em uma resposta.

— Inclua em seu plano de resposta ações de restrição imediata, quais stakeholders e autoridades legais devem ser informadas, como sua organização armazenará e restaurará informações com segurança a partir de backups e um local alternativo de onde atividades críticas para os negócios possam ser executadas durante a correção.

— Inclua em seu planejamento um cenário de roubo e fuga de dados como parte dos ataques de ransomware. Essa é uma tática comum muito usada atualmente e é executada em diversos ataques de ransomware remediados pela X-Force.

— Use simulações de ransomware para também decidir se sua empresa pagaria por um resgate e quais fatores teriam impacto sobre seus cálculos para tal decisão.

— Certifique-se de que seu plano de resposta ao ransomware inclua uma contingência específica para um incidente relacionado à nuvem, pois pode requerer ferramentas e habilidades adicionais.

— Evite a corrupção de dados devido a ataques de malware ou ransomware com soluções de armazenamento flash que ajudam a evitar perda de dados, promovem a continuidade das operações e geram menos custos de infraestrutura.

— O Definitive Guide to Ransomware da X-Force oferece mais orientações detalhadas sobre como responder a ataques de ransomware. A equipe de resposta a incidentes da X-Force também pode conduzir uma avaliação de prontidão contra ransomware em sua empresa para ajudar a elaborar e testar um plano de resposta a incidentes contra ransomware. O X-Force Command Center também prepara as organizações para um ataque de ransomware, levando em conta os requisitos de negócios e de resposta técnica.

**Implemente a autenticação multifator em cada ponto de acesso remoto da rede.** A X-Force observou que mais organizações implementaram a MFA com sucesso do que nunca. Isso está literalmente alterando o cenário de ameaças, forçando os agentes de ameaças a encontrar novas formas de comprometer as redes que não sejam usar credenciais roubadas e reduzindo a eficácia de campanhas de invasão de e-mail.

— A MFA pode reduzir o risco de vários tipos diferentes de ataque, incluindo ransomware, roubo de dados, BEC e acesso ao servidor.

— Além disso, as tecnologias de gestão de acesso e identidade estão facilitando a implementação de MFA a cada ano, tanto para equipes de implementação quanto para os usuários finais.

**Adote uma abordagem em camadas para combater o phishing.** Infelizmente, não existe uma ferramenta ou solução que possa evitar todos os ataques de phishing que existem atualmente, e os agentes de ameaças continuam a refinar as técnicas de detecção antimalware e a engenharia social para burlar os controles estabelecidos. Assim, recomendamos a implementação de várias camadas de soluções que oferecem maior probabilidades de capturar e-mails de phishing.

— Primeiro, a conscientização e o treinamento efetivos do usuário são fundamentais e devem incluir exemplos reais.

— Em segundo lugar, adote uma solução de segurança de software de e-mail, colocando uma máquina para assumir a tarefa de identificar e filtrar mensagens maliciosas.

— Terceiro, implemente várias defesas que possam ajudar a capturar atividades de malware ou de movimento lateral rapidamente caso um e-mail de phishing passe, incluindo detecção de malware baseada em comportamento, detecção e resposta de terminal (EDR), soluções de detecção e prevenção de Intrusão (IDPS) e um sistema de gerenciamento de eventos e informações de segurança (SIEM).

**Refine e amadureça seus sistema de gerenciamento de vulnerabilidade.** O gerenciamento de vulnerabilidades é uma arte, desde identificar quais vulnerabilidades são mais aplicáveis à arquitetura de rede da sua organização até identificar como implementá-las sem interromper nada no processo.

— Ter uma equipe dedicada ao gerenciamento e garantir que essa equipe receba bom suporte e recursos pode fazer toda a diferença para garantir que sua rede esteja protegida de possíveis explorações de vulnerabilidade.

— Recomendamos priorizar qualquer uma das vulnerabilidades mencionadas nesta avaliação que seja aplicável à sua empresa.

— O X-Force Exchange da IBM também inclui um repositório de vulnerabilidades e níveis de criticidade associados a elas para ajudá-lo a identificar as mais preocupantes, e o X-Force Red oferece serviços especializados de gerenciamento e verificação de vulnerabilidades.

Saiba mais no relatório completo →

# Sobre a IBM Security X-Force

A IBM Security X-Force é uma equipe de hackers, respondedores, pesquisadores e analistas centrada em ameaças. Nosso portfólio inclui produtos e serviços ofensivos e defensivos, alimentados por uma visão de 360 graus das ameaças. Com a X-Force como sua parceira de segurança, você pode afirmar com confiança que a probabilidade e o impacto de uma violação de dados são mínimos.

A IBM Security X-Force Threat Intelligence combina telemetria de operações de segurança da IBM, pesquisa, investigações de resposta a incidentes, dados comerciais e fontes abertas para ajudar os clientes a entenderem as ameaças emergentes e tomar decisões de segurança informadas rapidamente.

Além disso, a equipe de resposta a incidentes da X-Force oferece serviços de detecção, resposta, correção e prontidão para ajudar você a reduzir o impacto de uma violação de dados.

A X-Force combinada à experiência do IBM Security Command Center treina a sua equipe, dos analistas aos mais altos executivos, para estar pronta para a realidade das ameaças atuais. A equipe de hackers da IBM Security, a X-Force Red, oferece serviços de segurança, incluindo teste de invasão, gerenciamento de vulnerabilidade e simulação de adversários.

Ao longo do ano, os pesquisadores da IBM X-Force também fornecem pesquisas e análises contínuas em blogs, artigos, webinars e podcasts, destacando nossa visão sobre os agentes de ameaças avançadas, novos malwares e métodos de ataque. Além disso, fornecemos um grande conjunto de análises atuais e de ponta para clientes assinantes por meio de nossas soluções X-Force Threat Intelligence.

Agende uma consultoria com um de nossos especialistas da X-Force

# Sobre a IBM Security

A IBM Security trabalha com você para ajudar a proteger seus negócios com um portfólio avançado e integrado de produtos e serviços de segurança corporativa, habilitado com IA e com uma abordagem moderna para sua estratégia de segurança usando princípios de zero trust, ajudando você a prosperar em situações de incerteza. Alinhando sua estratégia de segurança à sua empresa, integrando soluções projetadas para proteger os usuários digitais, ativos e dados, e implementando tecnologia para gerenciar suas defesas contra ameaças crescentes, ajudamos você a gerenciar e controlar os riscos que atingem os ambientes de nuvem híbrida de hoje.

Nossa nova abordagem moderna e aberta, a plataforma IBM Cloud Pak for Security, foi desenvolvida com o RedHat Open Shift e oferece suporte aos atuais ambientes de multinuvem híbrida com um amplo ecossistema de parceiros. O Cloud Pak for Security é uma solução de software em contêiner desenvolvida para empresas que permite gerenciar a segurança de seus dados e aplicações, integrando rapidamente suas ferramentas de segurança existentes para gerar insights mais profundos sobre ameaças em ambientes de nuvem híbrida, mantendo seus dados onde estão, permitindo fácil orquestração e automação de sua resposta de segurança.

Para obter mais informações, visite www.ibm.com/br-pt/security ou o blog IBM Security Intelligence.

# Colaboradores

Camille Singleton
Charles DeBeck
Joshua Chung
Dave McMillen
Scott Craig
Scott Moore
Charlotte Hammond
John Dwyer
Melissa Frydrych
Ole Villadsen
Richard Emerson
Guy-Vincent Jourdan
Vio Onut
Stephanie Carruthers
Adam Laurie
Michelle Alvarez
Salina Wuttke
Georgia Prassinos
John Zorabedian
Mitch Mayne
Limor Kessem
Ian Gallagher
Ari Eitan

© Copyright IBM Corporation 2022

IBM Brasil Ltda
Rua Tutóia, 1157
CEP 04007-900
São Paulo – SP
Brasil

Produzido nos Estados Unidos da América em fevereiro de 2022

IBM, o logotipo da IBM e ibm.com são marcas comerciais da International Business Machines Corp., registradas em muitas jurisdições em todo o mundo. Outros nomes de produtos e serviços podem ser marcas comerciais da IBM ou outras empresas. Uma lista atualizada das marcas comerciais da IBM encontra-se disponível na web em “Copyright and trademark information” (“Informações de copyright e marca registrada”) no endereço ibm.com/legal/copytrade.shtml

Este documento estava atualizado na data de publicação inicial e pode ser alterado pela IBM a qualquer momento. Nem todas as ofertas estão disponíveis em todos os países onde a IBM opera. Os dados de desempenho e exemplos de clientes citados são apresentados apenas para fins ilustrativos. Os resultados de desempenho reais poderão variar, dependendo das configurações e das condições operacionais específicas.

AS INFORMAÇÕES NESTE DOCUMENTO SÃO OFERECIDAS NO ESTADO EM QUE SE ENCONTRAM (“AS IS”) SEM QUALQUER GARANTIA, EXPLÍCITA OU IMPLÍCITA, INCLUINDO SEM QUAISQUER GARANTIAS DE COMERCIABILIDADE, ADEQUAÇÃO A UM PROPÓSITO ESPECIAL E QUALQUER GARANTIA OU CONDIÇÃO DE NÃO VIOLAÇÃO.

Os produtos IBM são garantidos de acordo com os termos e condições dos acordos sob os quais são fornecidos. O cliente é responsável por garantir a conformidade com as leis e regulamentações aplicáveis. A IBM não fornece conselhos jurídicos e não declara ou garante que seus serviços ou produtos irão assegurar que o cliente está em conformidade com qualquer lei ou regulamento. As declarações referentes à orientação e intenção futuras da IBM estão sujeitas à mudança ou retirada sem aviso prévio e representam apenas metas e objetivos.