



Risco positivo na segurança cibernética

AWS Recomendações



AWS Recomendações: Risco positivo na segurança cibernética

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens de marcas da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestige a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

Introdução	1
Benefícios do risco positivo	3
Promover resultados positivos	3
Aumentar a postura de segurança	4
Alterando a linguagem de risco	5
Aumentar a adoção	6
Exemplos de risco positivo	7
Risco positivo em tecnologia	7
Risco positivo de gerenciamento de projetos	7
Risco positivo da segurança cibernética	7
Resposta ao risco de segurança cibernética	9
Próximas etapas	12
Perguntas frequentes	13
Risco desejável e risco positivo	13
Importância	13
Recursos	14
Histórico do documento	15
.....	xvi

Risco positivo na segurança cibernética

Greg Bell, Amazon Web Services (AWS)

Maio de 2022 ([histórico do documento](#))

A maioria das pessoas pensa no risco de uma perspectiva negativa, como exposição a perdas ou gerenciamento de eventos adversos. No entanto, a definição de risco da International Organization for Standardization (ISO) é o “efeito da incerteza nos objetivos”. Nesse caso, o efeito pode ser positivo ou negativo.

Os riscos reais podem variar entre os setores, mas essa definição padrão se aplica a todos eles, e cada setor tem seus riscos negativos e positivos. No setor de segurança cibernética, risco negativo refere-se a perdas potenciais e risco positivo refere-se ao ganho potencial em ativos, conhecimento, melhorias ou dados.

O gerenciamento de projetos e os domínios de TI adotaram a estratégia de avaliar riscos positivos em relatórios e decisões de negócios. No entanto, o setor de segurança cibernética ainda não adotou isso como uma prática comum, e muitas metodologias de gerenciamento de riscos continuam se concentrando nos riscos negativos. Se o risco positivo chega a ser discutido, isso é feito apenas brevemente.

Tradicionalmente, a segurança cibernética vê o risco exclusivamente através de uma lente negativa. A seguir estão os dois tipos comuns de risco negativo na segurança cibernética:

- Risco negativo: exposição a perdas causadas por fatores externos, como uma ameaça. Por exemplo, cibercriminosos podem introduzir ou aumentar a probabilidade de um incidente de segurança.
- Risco ascendente: exposição a perdas em busca de um ganho, como uma vulnerabilidade resultante da mudança. Por exemplo, ao implementar uma estratégia de TI, é possível aumentar inadvertidamente o potencial de um incidente de segurança. Risco desejável não é o mesmo que risco positivo. Mesmo que ele ocorra na busca por um ganho, o risco desejável está focado no potencial de perda.

Até recentemente, a segurança cibernética considerava apenas o risco negativo, e a definição de risco se concentrava em um possível resultado negativo. Os riscos positivos se concentram no resultado positivo potencial no início da identificação do risco. A exclusão do risco positivo resulta na falha em reconhecer os resultados positivos na segurança cibernética. Devido ao foco no risco

negativo, os líderes executivos geralmente percebem que a segurança cibernética é reativa em vez de proativa e subestimam a contribuição da segurança cibernética para resultados comerciais positivos.

Este documento define o risco positivo para o setor de segurança cibernética e discute os benefícios e a importância de incluir riscos positivos em sua estratégia de segurança cibernética.

Benefícios do risco positivo

Particularmente em um setor como o de segurança cibernética, que se concentra em proteger a empresa contra possíveis perdas, é fácil enquadrar o risco de uma perspectiva negativa. Reformular os riscos de segurança cibernética com base em seus ganhos potenciais pode beneficiar os negócios, promovendo resultados positivos, aumentando a postura de segurança da organização e aumentando a confiança do cliente.

Promover resultados positivos

A adoção de riscos positivos permite que a organização avalie e reconheça a contribuição que o domínio faz para resultados comerciais positivos. De acordo com [Segurança cibernética entre os executivos nível C e a sala de reuniões](#) (Relatório de pesquisa do Enterprise Strategy Group):

- 69% dos líderes de negócios e tecnologia acreditam que a segurança cibernética é total ou principalmente uma área de tecnologia com pouca ou nenhuma ligação com os negócios.
- 11% dos líderes de negócios e de tecnologia comparam a segurança cibernética à conformidade regulatória.
- 82% das organizações afirmam que os riscos de segurança cibernética aumentaram nos últimos dois anos devido a fatores como o aumento das ameaças cibernéticas, maior integração da tecnologia nos negócios e uma superfície de ataque crescente.

Quando os executivos de segurança cibernética integram riscos positivos em conversas e relatórios, isso ajuda a promover o valor das operações de TI seguras na empresa.

Por exemplo, digamos que uma empresa tenha sofrido uma violação de dados há vários anos causada pela falta de um processo de gerenciamento de patches. O incidente ainda é divulgado pela mídia e afeta as percepções e interações dos clientes com a empresa. A empresa quer superar o incidente e expandir suas ofertas de serviços, mas a confiança do cliente está prejudicando as vendas. A segurança cibernética usa riscos positivos para convencer a liderança a investir em um processo de gerenciamento de patches que atualiza continuamente as aplicações. O novo processo reduz drasticamente o risco de violação de dados, melhorando a postura de segurança da empresa. As notícias do processo de gerenciamento de up-to-the-minute patches chegam à mídia e aos clientes em potencial. Os clientes agora se sentem confortáveis para comprar da empresa e as vendas aumentam para um nível impressionante.

Deixar de considerar riscos positivos durante a identificação de riscos pode fornecer uma avaliação incompleta e afetar a decisão comercial. Para obter exemplos concretos de riscos positivos que podem afetar as decisões de negócios, consulte [Exemplos de risco positivo](#).

Aumentar a postura de segurança e a confiança do cliente

A segurança cibernética é parte integrante da postura de segurança da empresa. As violações de dados podem afetar negativamente a confiança do cliente, mas uma forte postura de segurança e reputação também podem aumentar a confiança do cliente e gerar oportunidades de negócios.

Conforme discutido em [Promover resultados positivos](#), pesquisas mostram que a liderança executiva compreende os riscos negativos associados à segurança cibernética, mas frequentemente não entende o risco positivo ou o valor comercial. No entanto, pesquisas mostram que a liderança na área de segurança cibernética entende como uma postura de segurança forte pode beneficiar a organização.

Em [Pesquisa sobre segurança cibernética: a aceleradora de inovações](#) (whitepaper da Vodafone), a Vodafone entrevistou 1.434 tomadores de decisão em segurança cibernética no mundo inteiro. De acordo com os dados obtidos:

- 73% dos entrevistados acreditam que uma segurança forte cria novas oportunidades de negócios.
- 89% disseram que melhorias na segurança aumentariam a fidelidade e a confiança do cliente.
- 90% também disseram que conseguiram melhorar sua imagem, alcançar novos clientes em potencial e também transformá-los em clientes reais.
- 89% acreditam que ter uma segurança cibernética eficaz é uma vantagem competitiva relevante que os ajuda a se diferenciar de seus concorrentes.
- 24% relataram um aumento nas receitas usando tecnologias de nuvem e Internet das Coisas (IoT) e adotando controles de segurança de TI direcionados.
- Em vez de usar possíveis resultados negativos ao se comunicar com a liderança executiva, você também pode usar o risco positivo para comunicar o valor comercial resultante de melhorar a confiança do cliente. Os executivos podem ser cautelosos ao financiar programas. Em alguns casos, a segurança cibernética obtém o mínimo necessário para funcionar. A comunicação interna dos riscos positivos nas solicitações de orçamento pode ajudar sua liderança a entender o valor comercial da segurança cibernética. Isso pode resultar orçamentos maiores para iniciativas de segurança cibernética e gerar receita para a empresa.

Alterar a linguagem de riscos em segurança cibernética

Parte do desafio de adotar o risco positivo para a segurança cibernética é que a terminologia técnica e específica do domínio se concentra no risco negativo, como ameaças, vulnerabilidades e controles de segurança. O setor de segurança cibernética deve evoluir e expandir seu vocabulário para incluir uma linguagem que enfatize os resultados comerciais positivos (ou riscos positivos) que a segurança cibernética traz para a empresa. Termos como vantagem comercial, benefícios e valor comercial destacam a contribuição da segurança cibernética para a organização.

Mudar a linguagem da segurança cibernética ajuda a mudar a percepção de que a segurança cibernética é uma área de tecnologia focada exclusivamente em ameaças e vulnerabilidades e não está atrelada aos negócios. A liderança empresarial geralmente subestima a contribuição da segurança cibernética para resultados comerciais positivos. Para obter mais informações sobre a percepção da liderança sobre a segurança cibernética, consulte [Promover resultados positivos](#).

Aumentar a adoção em áreas relacionadas

Há um interesse crescente em muitos campos em incluir riscos positivos porque ele reconhece as contribuições que o domínio faz aos resultados comerciais. O conceito de risco positivo foi recentemente adotado em processos e definições comuns de gerenciamento de projetos.

Em 2013, o Project Management Institute (PMI) incorporou a definição de risco positivo (também chamado oportunidades) na quinta edição do Project Management Body of Knowledge (PMBOK). O PMBOK define risco individual como “um evento ou condição incerta que, se ocorrer, causará um efeito positivo ou negativo em um ou mais objetivos do projeto”. Ele define o risco do projeto geral do projeto como “o efeito da incerteza no projeto como um todo... mais do que a soma dos riscos individuais dentro de um projeto, uma vez que inclui todas as fontes de incerteza do projeto... representa a exposição das partes interessadas às implicações das variações no resultado do projeto, tanto positivas quanto negativas”.

Infelizmente, a inclusão de resultados positivos pelo PMI em suas definições de risco ainda não se aplica ao setor de segurança cibernética.

Exemplos de risco positivo

A seguir estão alguns exemplos de risco positivo para tecnologia, gerenciamento de projetos e segurança cibernética.

Risco positivo em tecnologia

Um exemplo de risco positivo em tecnologia é que a implementação de uma tecnologia poderia levar a uma redução do custo representado pelos salários. Por exemplo:

1. A implementação da tecnologia pode levar a uma maior eficiência nos negócios.
2. Essas eficiências podem gerar uma redução na quantidade de mão de obra.
3. A redução da mão de obra pode levar à redução do custo dos salários.

Risco positivo de gerenciamento de projetos

Um exemplo de risco positivo no gerenciamento de projetos é que o erro de cálculo do orçamento de um projeto pode levar à redução de custos ou ao financiamento de projetos adicionais. Por exemplo:

1. A implementação precoce de um projeto de tecnologia pode resultar no cálculo incorreto dos custos do projeto pelo gerente.
2. O cálculo incorreto dos custos do projeto pode levar ao excesso de fundos para o projeto.
3. O excesso de fundos para um projeto pode levar à redução de custos ou ao financiamento de projetos adicionais.

Risco positivo da segurança cibernética

Um exemplo de risco positivo na segurança cibernética é que a implementação do gerenciamento de patches pode aumentar a confiança do cliente. Por exemplo:

1. A implementação do gerenciamento de patches pode reduzir as vulnerabilidades em uma aplicação.
2. A remoção de vulnerabilidades pode reduzir os riscos da aplicação e torná-la mais segura.
3. A segurança aprimorada da aplicação pode reduzir a perda de dados.

4. A redução da perda de dados pode aumentar a confiança do cliente.

Outro exemplo de risco positivo na segurança cibernética é que a implementação da resposta a incidentes pode aumentar a produtividade dos funcionários. Por exemplo:

1. A implementação da resposta a incidentes pode levar à detecção de um aumento no tráfego de rede.
2. O aumento no tráfego de rede pode levar à detecção do uso indevido de recursos pelos funcionários acessando conteúdo não relacionado ao trabalho, como serviços de streaming de música e vídeo. Essas atividades consomem largura de banda da rede e podem afetar negativamente a performance da rede e das aplicações.
3. A detecção do uso indevido dos recursos da empresa pelos funcionários pode levar ao bloqueio desses serviços.
4. O bloqueio desses serviços pode reduzir o consumo de largura de banda da rede e aumentar a produtividade dos funcionários.

Por fim, o último exemplo de risco positivo em segurança cibernética é que a implementação de um plano de resposta a incidentes pode aumentar as oportunidades de negócios e a conformidade com as leis de privacidade. Por exemplo:

1. A implementação de um plano de resposta a incidentes pode levar a detecção e a identificação rápidas de malware e ransomware.
2. A identificação de malware e ransomware poderia minimizar o impacto e mitigar a ameaça aos recursos da empresa.
3. Mitigar a ameaça aos recursos da empresa pode levar a novas oportunidades de negócios e ajudar a empresa a permanecer em conformidade com as leis de privacidade.

Resposta ao risco de segurança cibernética

As respostas aos riscos positivos e aos riscos negativos são muito diferentes. Para os riscos negativos, é necessário adotar medidas para minimizar o impacto no resultado, mas para os riscos positivos, você deve tomar medidas para maximizar o impacto no resultado. A tabela a seguir mostra as possíveis respostas a riscos positivos e negativos.

Tipo de tarefa	Resposta	Definição
Risco positivo	Explorar	Maximize a probabilidade ou a possibilidade de o risco ocorrer para obter seu efeito positivo.
	Compartilhar	Aloque parte da propriedade de ou responsabilidade pelo risco a outra parte. Essa é a mesma abordagem de um risco negativo e tenta controlar perdas ou ganhos potenciais.
	Melhorar	Aumente as condições que geram risco para maximizar a oportunidade.
	Ignorar	Ignore a possibilidade do risco e não tome nenhuma ação. Essa resposta é comum quando a probabilidade do risco é muito baixa ou quando os benefícios de um possível resultado positivo são mínimos.
Risco negativo	Mitigar	Minimize a probabilidade ou a possibilidade de o risco ocorrer.

Tipo de tarefa	Resposta	Definição
	Transferir	Transfira a responsabilidade pelo risco para outra parte, como comprar uma apólice de seguro para transferir o risco para uma seguradora.
	Evitar	Elimine as condições que criam o risco.
	Aceitar	Reconheça a existência do risco, mas não tome nenhuma ação.

Para riscos negativos, as organizações evitam, transferem, mitigam ou aceitam o risco com base em sua tolerância ao risco e apetite. Elas tentam evitar que o risco ocorra e, quando ele ocorre, tentam minimizar seu impacto na missão geral.

A melhor maneira de ilustrar as respostas positivas ao risco é usar exemplos:

- Explorar: um executivo de segurança descobre que um profissional de segurança bem qualificado decidiu recentemente procurar um novo emprego e organiza um generoso bônus de assinatura para atrair o possível funcionário para sua equipe.
- Compartilhar: um líder de unidade de negócios gostaria de melhorar a segurança usando um produto de gerenciamento de acesso privilegiado, mas não tem um orçamento suficiente para comprar as ferramentas e os serviços no ano fiscal atual. O líder trabalha com um líder de uma unidade de negócios diferente que comprará e implementará a ferramenta como um projeto piloto e, posteriormente, expandirá a instalação para oferecer suporte às duas unidades de negócios.
- Melhorar: um funcionário identificou uma oportunidade de automatizar um processo comercial existente para reduzir as ameaças à segurança cibernética, mas isso exige investimentos em tempo e equipamento. Percebendo os benefícios positivos desse processo, o gerente aprova horas extras de trabalho para desenvolver a capacidade e redireciona recursos de hardware e software existentes para permitir que o projeto avance.
- Ignorar: um executivo financeiro descobre que um funcionário que trabalha no departamento de vendas desenvolveu uma nova aplicação que automatiza uma tarefa tediosa e manual. Recentemente, a aplicação foi autorizada para uso somente no departamento de vendas. O

executivo financeiro obtém uma cópia da nova solicitação para obter uma vantagem semelhante em seu departamento, sem autorização explícita.

Próximas etapas

Os domínios de tecnologia e gerenciamento de projetos adotaram riscos positivos em seus processos de avaliação de riscos, mas o setor de segurança cibernética historicamente os excluiu. Riscos positivos podem resultar em resultados comerciais positivos, e o setor de segurança cibernética deve fazer a transição para abraçar riscos positivos e obter os benefícios.

Você pode começar a comunicar riscos positivos imediatamente em todas as comunicações. Por exemplo, avaliações de risco, avaliações de segurança ou relatórios de status devem incluir uma seção sobre riscos positivos. As solicitações de financiamento à liderança executiva devem incluir riscos positivos, comunicar os benefícios potenciais para a empresa e destacar quaisquer vantagens comerciais potenciais obtidas com a aprovação da solicitação.

Perguntas frequentes

Qual é a diferença entre risco bom e risco positivo?

Ainda que os termos risco desejável e risco positivo soem semelhantes, na verdade eles são conceitos muito diferentes. Dentro do risco, há um resultado positivo ou negativo, e entre os resultados negativos, há um lado bom ou um lado ruim.

Risco positivo é o ganho potencial de ativos, conhecimento, melhorias ou dados. Por exemplo, você implementa rapidamente o gerenciamento de patches e um processo para remover vulnerabilidades, por exemplo, em uma semana. Ao longo do ano seguinte, não haverá incidentes de segurança.

Risco desejável é a exposição à perda durante a busca por um ganho. Por exemplo, a empresa implementa uma nova aplicação, enquanto você implementa rapidamente o gerenciamento de patches e um processo para remover vulnerabilidades, por exemplo, em uma semana. A exposição à perda (o período de tempo em que você remove as vulnerabilidades) ocorre em busca de um ganho (uma aplicação mais seguro), portanto, isso é considerado um risco desejável. É possível aumentar o risco desejável alterando o processo para remover vulnerabilidades para um dia ou diminuir o risco desejável alterando esse período para um mês. Basicamente, o risco desejável é a possibilidade incerta de ganho ao tentar minimizar uma perda.

Por que é importante incluir riscos positivos na segurança cibernética?

A integração de riscos positivos nas avaliações e conversas de risco de segurança cibernética ajuda a promover o valor da segurança cibernética para os negócios. Para obter mais informações, consulte [Benefícios do risco positivo](#).

Recursos

- [Segurança cibernética entre os executivos nível C e a sala de reuniões](#) (Relatório de pesquisa do Enterprise Strategy Group)
- [Pesquisa sobre segurança cibernética: o acelerador da inovação](#) (whitepaper da Vodafone)
- [Integração da segurança cibernética e gerenciamento de riscos corporativos \(ERM\)](#) (publicação do NIST)
- [Diferença entre riscos “desejados” e riscos “positivos”](#) (publicação no blog do instituto FAIR)

Histórico do documento

A tabela a seguir descreve alterações significativas feitas neste guia. Se desejar receber notificações sobre futuras atualizações, inscreva-se em um [feed RSS](#).

Alteração	Descrição	Data
Publicação inicial	—	27 de maio de 2022

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.