

Dezembro de 2022

# Estado da Segurança Física 2022:

**Navegando efetivamente por um  
cenário de mudanças**

Insights da pesquisa com mais de 3.700  
profissionais de segurança física

**Genetec**<sup>TM</sup>



# Conteúdo



<b>Sobre a pesquisa</b>	<b>2</b>
<b>Sumário executivo</b>	<b>4</b>
<b>Resumo das diferenças ao redor do mundo</b>	<b>5</b>
<b>Principais conclusões</b>	<b>7</b>
Os orçamentos OPEX crescem	7
TI desempenha um papel maior na segurança física	8
Competindo por componentes	9
Os recursos humanos enfrentam muitos desafios	11
Observações sobre a adoção da nuvem	13
A segurança física e os dados relacionados são vitais	18
Cybersecurity ainda é a principal prioridade	20
A segurança física torna-se unificada	22
Mudanças na tecnologia – o ano passado	23
Mudanças na tecnologia – o ano à frente	23
<b>Principais aprendizados</b>	<b>25</b>
<b>Apêndice</b>	<b>27</b>
Apêndice 1 - Metodologia de pesquisa	27
Apêndice 2 - Informações demográficas da pesquisa	28
Apêndice 3 - Comentários abertos	30

# Sobre a pesquisa



A Genetec Inc. entrevistou profissionais de segurança física de 24 de agosto a 21 de setembro de 2022. Após a filtragem dos dados e uma revisão das entrevistas, 3.711 respostas foram incluídas na amostra para análise.

## Alguns detalhes sobre a metodologia de pesquisa

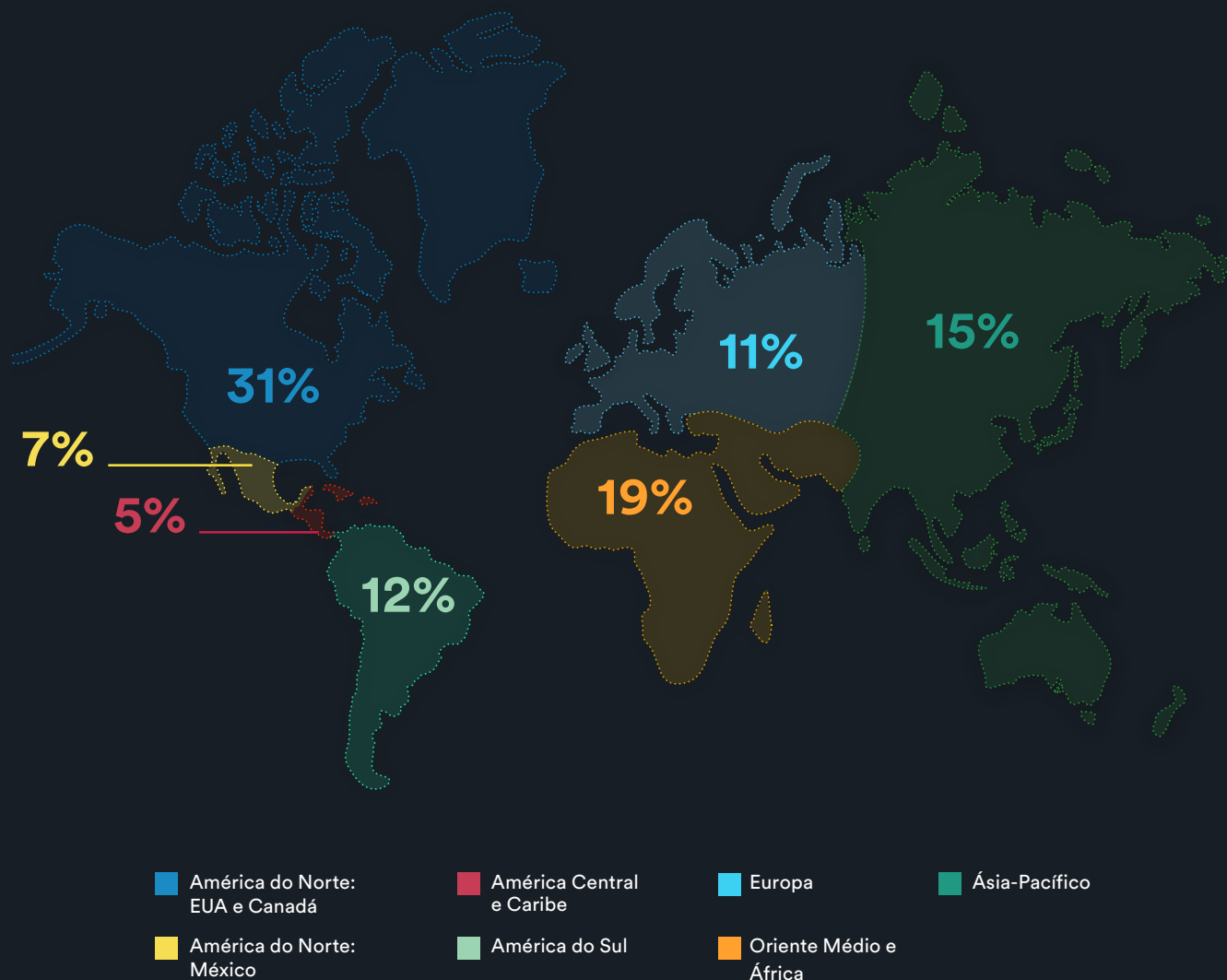
O público-alvo da pesquisa focou em dois grupos principais:

- **Usuários finais** (indivíduos que trabalham para organizações que participam da aquisição, gerenciamento e/ou uso de tecnologia de segurança física) e
- **Integradores, instaladores e fornecedores de sistemas** (indivíduos que prestam consultoria, integram, instalam, vendem ou prestam serviços voltados a soluções de segurança)

O público-alvo foi alcançado através de terceiros por meio de suas listas de e-mail opt-in, listas de e-mail opt-in da Genetec e promoções digitais. Alguns dos resultados deste relatório são baseados em respostas de usuários finais e integradores/instaladores/fornecedores de sistemas. No entanto, algumas perguntas foram feitas apenas para usuários finais e outras apenas para integradores/instaladores/fornecedores de sistemas. Este relatório aponta se as respostas são de todos os entrevistados, usuários finais ou integradores/instaladores/fornecedores de sistemas.

Mesmo para as perguntas feitas a ambos os grupos (usuários finais e integradores/instaladores/fornecedores de sistemas), cada resultado foi analisado pelas respostas de 'somente usuários finais' e 'somente integradores/instaladores/fornecedores de sistemas', bem como por ambos os grupos combinados. Na maioria dos casos, houve pouca diferença nos resultados. As respostas de 'somente usuários finais' estavam de acordo com as respostas de 'somente integradores/instaladores/fornecedores de sistemas'. O relatório aponta casos em que esse não foi o caso. Ele também aponta casos em que a porcentagem de respostas difere significativamente por região geográfica, setor de usuário final ou tamanho da organização, medido pelo número de colaboradores globais.

As amostras incluem público-alvo de todas as regiões geográficas.



Apenas pesquisas totalmente preenchidas por indivíduos dentro do público-alvo foram incluídas na análise final. Para mais detalhes sobre a metodologia da pesquisa e dados demográficos dos participantes, consulte os Apêndices 1 e 2.

# Sumário executivo



As organizações estão fazendo um balanço e adotando uma nova maneira de trabalhar após um período de incerteza e mudança impulsionado pela pandemia do COVID-19. Muitos dos resultados da pesquisa de 2022 foram semelhantes às respostas da [pesquisa de 2021](#). Mas alguns destes resultados também revelaram novos desafios enfrentados pelo setor, como escassez de produtos e problemas com recursos humanos.

O que está claro é que as organizações estão prontas e aptas para se adaptar e estão olhando para o futuro quando se trata da aplicação da tecnologia de segurança física:



**O futuro da nuvem é híbrido:** Muitas organizações vislumbram uma combinação de soluções in loco e hospedadas na nuvem para suas implantações de segurança física, à medida que buscam otimizar seus investimentos em infraestrutura e alavancar opções híbridas para economizar custos e aumentar a eficiência.



**A influência da cybersecurity e da TI:** As preocupações cibernéticas estão aumentando e inspirando novos métodos para implementar e manter uma forte estratégia de cybersecurity.



**O uso de segurança física para operações comerciais:** A pandemia levou mais organizações a aproveitar vários sistemas e fontes de dados para gerenciar melhor suas instalações e o fluxo de pessoas. A tendência de considerar as soluções de segurança física como mais do que apenas um custo associado à proteção de pessoas e ativos continuará e novas abordagens de como os dados de segurança física são usados informarão as decisões organizacionais e operacionais.



**Superando a escassez de suprimentos:** A indústria se adaptou aos problemas da supply chain, ampliando o valor de seu hardware existente ou atrasando projetos. Com os orçamentos de 2023 permanecendo saudáveis, os departamentos de segurança e TI estão planejando concluir as implantações ou iniciar novos projetos à medida que os componentes se tornam prontamente disponíveis.

# Resumo das diferenças ao redor do mundo



Para a maioria das perguntas em nossa pesquisa, houve pequenas diferenças entre os entrevistados regionais. Ou seja, a porcentagem de respostas para cada resposta e cada região foi semelhante. Isso sugere uma visão global consistente de como a segurança física se desenvolveu no último ano.

Abaixo estão os casos em que as respostas de uma região específica diferiram significativamente da média global.

## 📍 **Ásia-Pacífico: supply chain e nuvem**

Os integradores de sistemas da Ásia-Pacífico estão mais pessimistas sobre o impacto dos problemas com a supply chain no próximo ano. 57,5% responderam que os problemas na supply chain iriam “aumentar muito” ou “aumentar um pouco”. Isso fica acima da média global de 49%.

Os entrevistados foram solicitados a atribuir uma classificação aos diferentes motivos para uma adoção lenta da nuvem. No geral, “riscos percebidos de cybersecurity” tem a classificação média mais alta. Na Ásia-Pacífico, o mais alto é “medo da perda de dados” seguido de perto por “falta de compreensão da nuvem”.

A região da Ásia-Pacífico está à frente no uso de nuvem privada. A maioria dos entrevistados globalmente ainda guarda seus vídeos em dispositivos de armazenamento in loco (por exemplo, NVRs, servidores, NAS, SAN). Na Ásia-Pacífico, 4,55% disseram que armazenaram seus dados de vídeo “principalmente em uma nuvem privada”, foi o mais alto entre todas as regiões.

## 📍 **América Central e Caribe: Unificação e nuvem**

Sistemas de segurança unificados são menos comuns na América Central e Caribe. “Os sistemas de videomonitoramento e controle de acesso da minha organização não estão conectados (são sistemas separados)” foi a segunda resposta mais comum escolhida. Em todas as outras regiões, essa foi a resposta menos comum.

Os entrevistados da América Central e Caribe também indicaram que usam armazenamento em nuvem pública com mais frequência do que em outras regiões. 6,9% dos entrevistados da América Central e Caribe responderam “principalmente através de serviços de armazenamento em nuvem pública” em comparação com 2,6% globalmente.

### 📍 Europa, Oriente Médio, Turquia e África: Nuvem, ameaça a credenciais e supply chain

A EMEA é a região mais conservadora quando se trata de adoção da nuvem para segurança física. 69% dos entrevistados afirmaram que não migraram nenhuma de suas infraestruturas para a nuvem, em comparação com uma média global de 58%.

Os entrevistados da EMEA confirmaram que o “roubo de credenciais” é a maior ameaça para suas organizações, com 50,2% escolhendo essa opção contra 39,6% globalmente.

A Europa sofreu os maiores desafios com a entrega de projetos nos últimos 12 meses, com 82% dos entrevistados afirmando que foram afetados, em comparação com 71% globalmente. Isso pode ser atribuído a reduções de orçamento e problemas na supply chain. Apesar desses desafios, os entrevistados afirmaram que a maioria dos projetos não foram cancelados, mas adiados para 2023.

### 📍 México: Nuvem

Apenas 17,4% dos entrevistados do México sugeriram que o COVID-19 acelerou um pouco sua estratégia de nuvem. Isso se compara a 30,9% globalmente. Também tiveram a menor parcela de entrevistados (29,4%) indicando que foi “um pouco” ou “muito” acelerado, em comparação com 46,7% globalmente e 47,9% nos EUA e Canadá juntos.

O México também indicou que o COVID-19 “desencadeou” sua estratégia de nuvem com mais frequência do que qualquer outra região (9,8%). Um forte contraste com os EUA e o Canadá, onde apenas 0,35% dos entrevistados disseram isso (de longe o menor entre todas as regiões).

### 📍 América do Sul: trabalho remoto e cybersecurity

50,4% dos entrevistados da América do Sul disseram que suas organizações não têm equipe de segurança física preparada para trabalhar remotamente, enquanto a média global é de 33,7%.

Eles também eram os menos propensos a identificar “melhor estratégia de cybersecurity” como um dos novos processos que priorizaram este ano. Apenas 38% dos entrevistados disseram isso, em comparação com 49,2% globalmente e 52,9% nos EUA e Canadá.

### 📍 EUA e Canadá: menos demissões, leitura de temperatura e unificação

41% dos entrevistados nos EUA e Canadá indicaram que “nenhum” de seus colaboradores de segurança foi demitido em 2021. Isso se compara a 29% globalmente.

A tecnologia de leitura de temperatura foi escolhida com menos frequência pelos entrevistados dos EUA e Canadá do que por todas as outras regiões, 14% contra 24% globalmente.

A unificação de sistemas de vídeo e controle de acesso foi a segunda mais comum nos EUA e no Canadá, com 80% dos entrevistados indicando que seus sistemas foram unificados em comparação com 77% globalmente.

# Principais conclusões

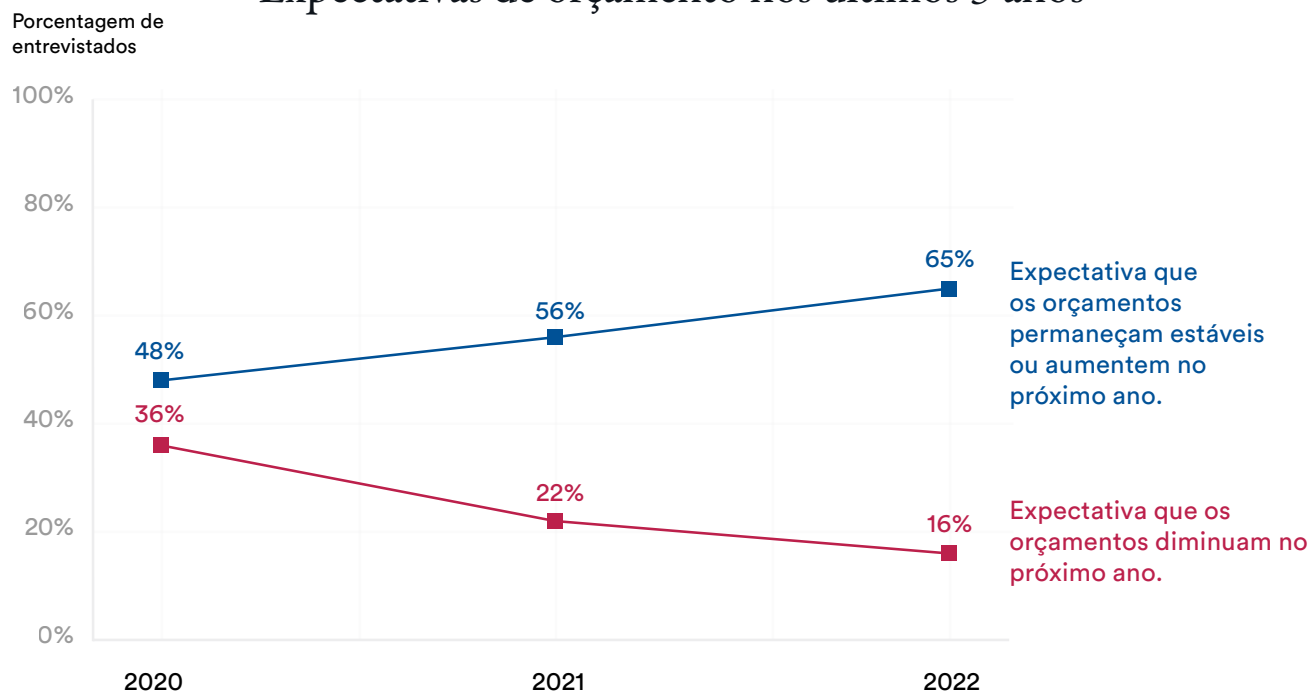


## Os orçamentos OPEX crescem

Com uma perspectiva econômica desafiadora para 2023, que prevê uma recessão em muitos países, é importante observar que em recessões e períodos de recessão anteriores, o mercado de segurança física continuou crescendo. Essa resiliência parece se refletir nos resultados da pesquisa, com as perspectivas gerais para os orçamentos OPEX permanecendo positivas para 2023 e continuando a se recuperar das consequências da pandemia:

### ORÇAMENTOS OPERACIONAIS

#### Expectativas de orçamento nos últimos 3 anos



Dadas as diferentes condições econômicas em todo o mundo, as respostas a esta pergunta não variaram significativamente por região. Isso reflete uma visão geral otimista em todo o setor de segurança física.



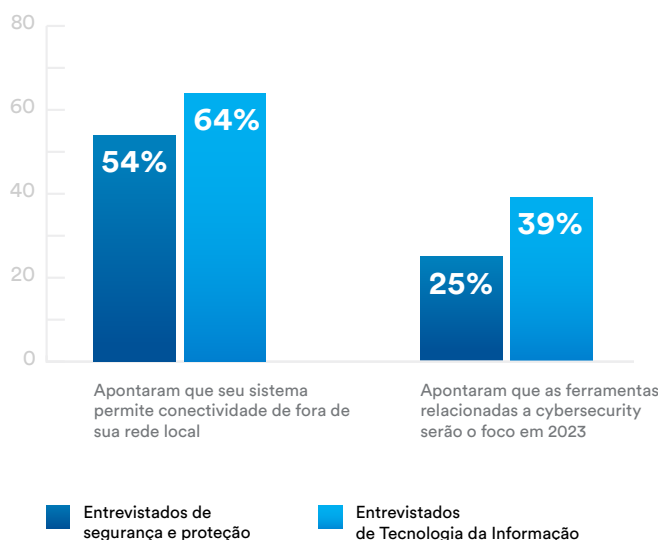
## TI desempenha um papel maior na segurança física

Há uma década, a maioria dos sistemas de segurança física em organizações maiores era gerenciada por colaboradores de departamentos de segurança especializados. No entanto, a transição para sistemas de segurança física de rede significou que os departamentos de Tecnologia da Informação (TI) estão assumindo maior responsabilidade pelo gerenciamento de sistemas de segurança física como parte da governança de rede e tecnologia. Não é nenhuma surpresa que em nossa pesquisa de 2022, os entrevistados que identificaram sua função de trabalho como “Tecnologia da Informação” tivessem um ponto de vista diferente de seus colegas que selecionaram “Segurança e Proteção”. As questões de rede e cybersecurity foram priorizadas nas respostas dos entrevistados de “Tecnologia da Informação” relacionadas ao gerenciamento e implantação desses sistemas de segurança física.



### TI VERSUS SEGURANÇA

#### Priorizando ferramentas de cybersecurity



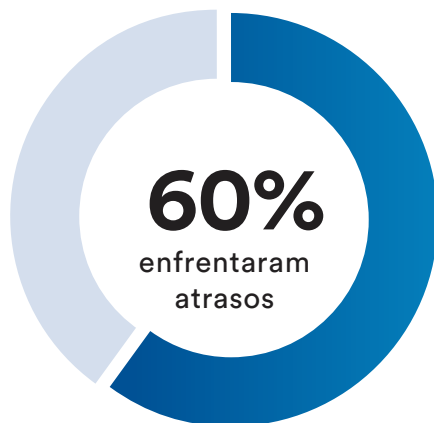
Os entrevistados de TI veem ransomware, engenharia/phishing e ataques de execução remota como uma ameaça maior para sua organização do que os entrevistados de Segurança e Proteção.

## Competindo por componentes

Em 2021, houve regras e restrições por conta da pandemia, além de desafios nas fábricas de Taiwan, bloqueios no Canal de Suez e dificuldades nos portos de entrada. Combinado com um aumento maciço na demanda de componentes em todos os setores (como fabricantes de smartphones e automóveis) e as novas necessidades “em casa” dos consumidores, isso levou a uma escassez sem precedentes de hardware de segurança física e atrasos nos projetos.



Os resultados da pesquisa demonstram os efeitos generalizados dos problemas da supply chain e como os profissionais de segurança física trabalharam pragmaticamente para administrá-los.



**60% dos usuários finais** apontaram que projetos de segurança física foram adiados devido a questões da supply chain. Muitos dos atrasos duraram longos períodos.

- 46% dos usuários finais enfrentaram mais de 3 meses de atrasos.
- 28% dos usuários finais enfrentaram mais de 6 meses de atrasos.

Muitos tipos diferentes de projetos foram adiados. Para os usuários finais que enfrentaram atrasos, a substituição de tecnologia ou equipamento foi a mais difícil (66%), seguida pela expansão das instalações atuais (51%) e atualizações (51%).

Para fornecedores de hardware de videomonitoramento, os atrasos tiveram sérias implicações, pois 45% dos usuários finais procuraram alternativas e mudaram de marca para implantar os equipamentos disponíveis.

Os integradores de sistemas também destacaram a necessidade de tentar diferentes estratégias para lidar com a escassez de hardware, incluindo o uso de “equipamento de segunda mão” e “um centro de reparos para trazer de volta para a produção alguns eletrônicos fáceis de consertar”.

# Ponto de vista



A crise do COVID-19 e o impacto subsequente na disponibilidade de hardware e componentes eletrônicos destacaram o papel crítico que a supply chain e a logística desempenham na maioria dos setores.

Embora a pandemia tenha ficado para trás, a nova situação socioeconômica e a incerteza desencadeada pelos atuais conflitos geopolíticos continuam pressionando a supply chain global.

Para o setor de segurança, isso se traduz em integradores de sistemas que precisam:

- Continuar fazendo pedidos de hardware bem antes dos projetos para garantir seu material quando necessário
- Desenvolver relacionamentos mais próximos com parceiros que possam fornecer alternativas potenciais para produtos de pedidos pendentes
- Associar-se a fornecedores que são resilientes e adaptáveis e que podem reprojetar rapidamente seus produtos com base na disponibilidade de matérias-primas e componentes

Temos uma previsão otimista de que os primeiros indicadores apontam para a redução dos gargalos da supply chain em 2023, o que deve fornecer o alívio necessário para os integradores de sistemas que buscam implantar novos projetos em tempo hábil.



**Nadia Boujenoui**  
Vice-presidente da Experiência do Cliente  
Genetec Inc.

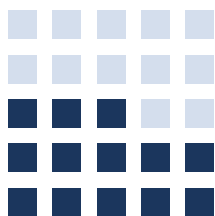
## Os recursos humanos enfrentam muitos desafios

Em todos os setores, a escassez de talentos, os planos de retorno à empresa e as expectativas dos colaboradores em relação a novas formas de trabalho desafiaram as organizações nos últimos dois anos. Os resultados da pesquisa demonstraram que o setor de segurança física não foi diferente.

50% de todos os entrevistados da pesquisa de 2022 indicaram que sua organização de segurança física enfrentou desafios de RH no ano passado. Os entrevistados comentaram que os desafios resultaram na necessidade de substituir e realocar colaboradores e que o tempo e o orçamento para treinamento eram limitados.

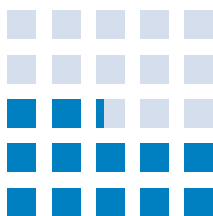


Para os entrevistados que enfrentaram tais desafios:



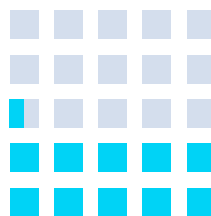
**52%**

Enfrentaram escassez de pessoal



**49%**

Enfrentaram dificuldades de contratação



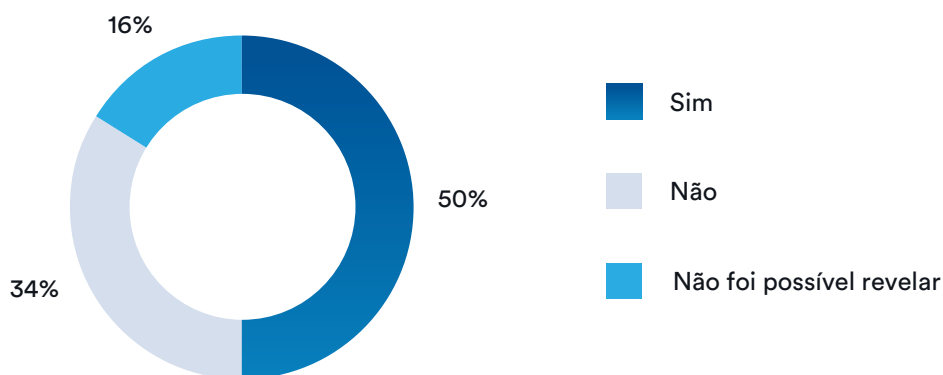
**42%**

Enfrentaram problemas com o ânimo dos funcionários

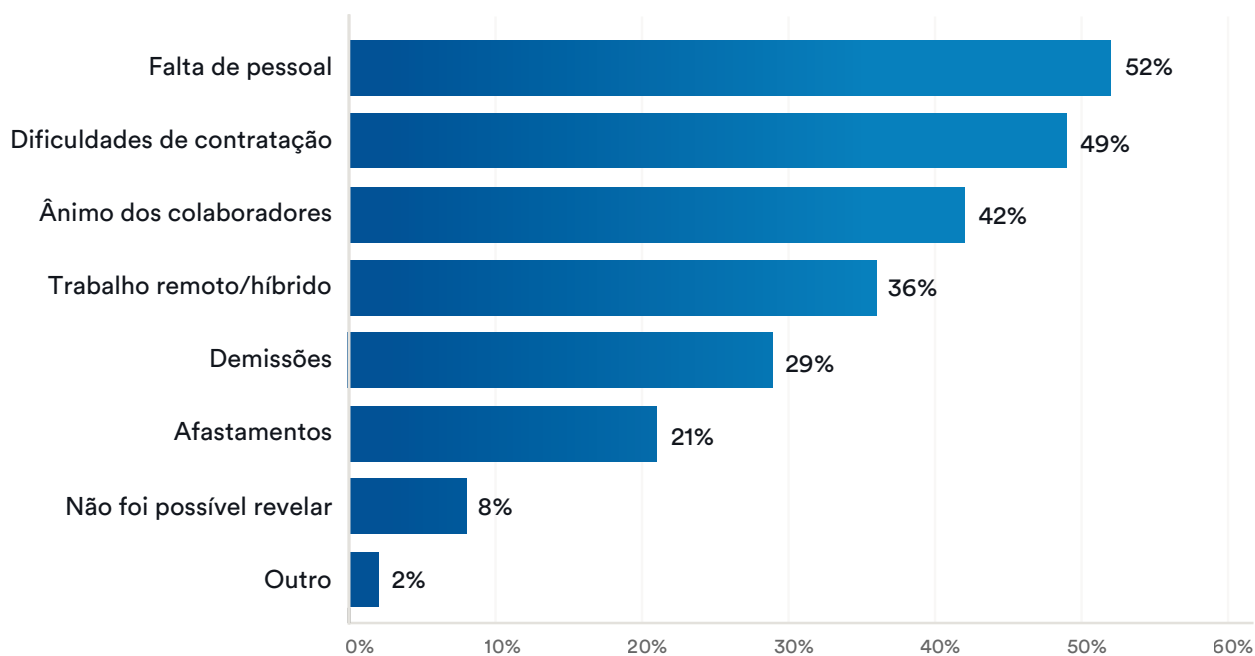
A pesquisa revelou que dos 48% que priorizaram o quesito acima, 83% são do setor de cannabis e 73% são do setor de jogos.

## OS RECURSOS HUMANOS ENFRENTAM MUITOS DESAFIOS

A sua organização de segurança física  
experienciou desafios de RH no último ano?



Que tipo de desafios de RH afetaram seu  
departamento de segurança física no último ano?



## Observações sobre a adoção da nuvem

### Aceitação da nuvem por região

A maioria dos usuários finais entrevistados (82%) indicou que salva principalmente imagens de vídeo em dispositivos de armazenamento locais (por exemplo, NVRs, servidores, NAS, SAN). Apenas 6% indicaram que usam nuvem pública ou privada para esse fim. O principal norteador é aproveitar o trabalho remoto, o que faz sentido, pois menos pessoas estão indo à empresa regularmente.

A porcentagem foi maior no setor de usuário final de varejo, onde 81% dos entrevistados indicaram que fariam a mudança para a nuvem. Além disso, uma porcentagem menor de entrevistados na Europa e no Oriente Médio achou que sua organização passaria a gerenciar ou armazenar seus dados de segurança física na nuvem do que em outras regiões.

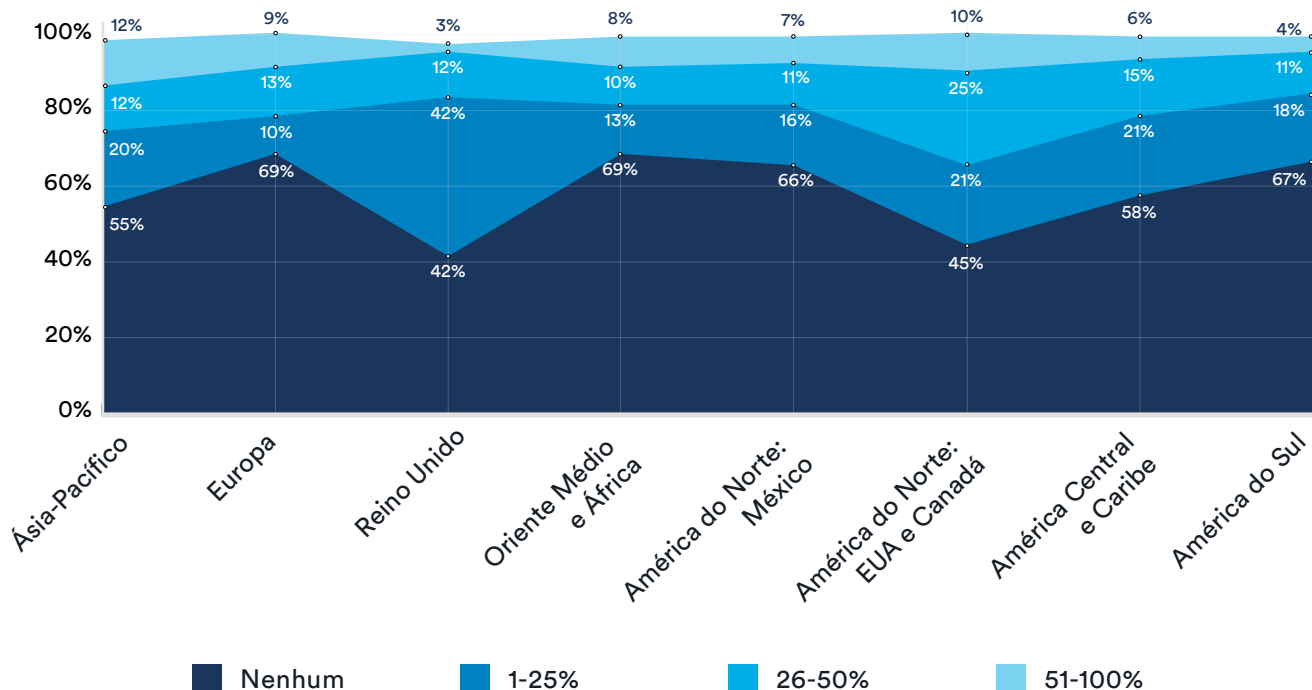


### Quase 2/3

de todos os entrevistados indicaram que, durante os próximos dois anos, sua organização passará a gerenciar ou armazenar mais dados de segurança física na nuvem.

#### OBSERVAÇÕES SOBRE A ADOÇÃO DA NUVEM

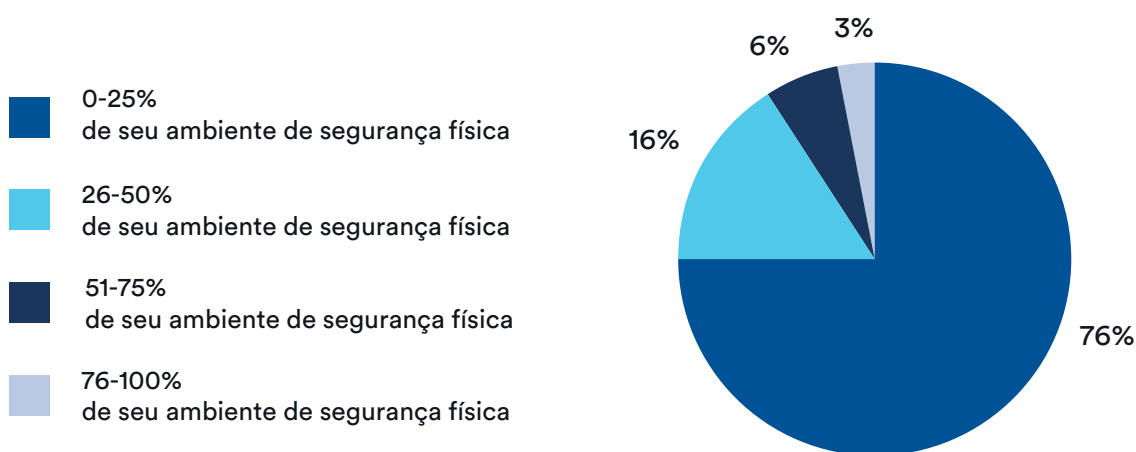
### Adoção de nuvem ou nuvem híbrida por região





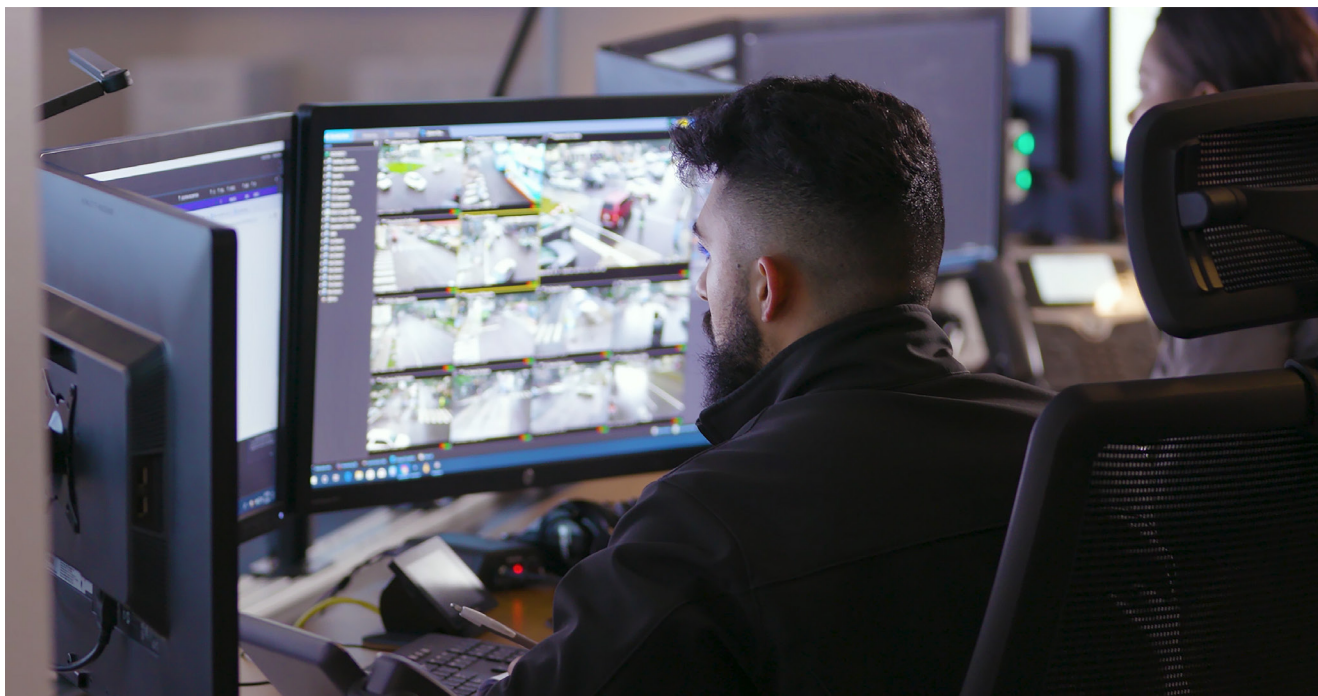
## OBSERVAÇÕES SOBRE A ADOÇÃO DA NUVEM

Quanto do seu ambiente de segurança física está na nuvem ou nuvem híbrida? (Escolha um)



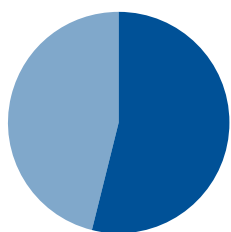
Esse movimento para a nuvem é consistente com as previsões dos analistas do setor.

A [Novaira Insights](#) informou que, nas Américas, a porcentagem das receitas de software para gerenciamento de vídeo provenientes de software de gerenciamento de vídeo na nuvem crescerá de 19% em 2021 para 45% em 2026.



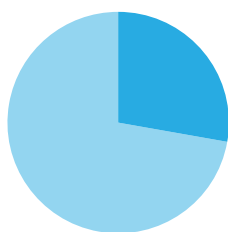
OBSERVAÇÕES SOBRE ADOÇÃO DA NUVEM

## O futuro tem cara de híbrido



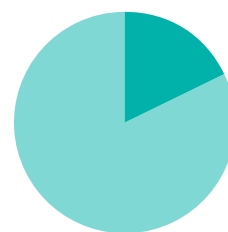
**54%**

de usuários finais apontaram que estão na direção de uma combinação de soluções in loco e na nuvem



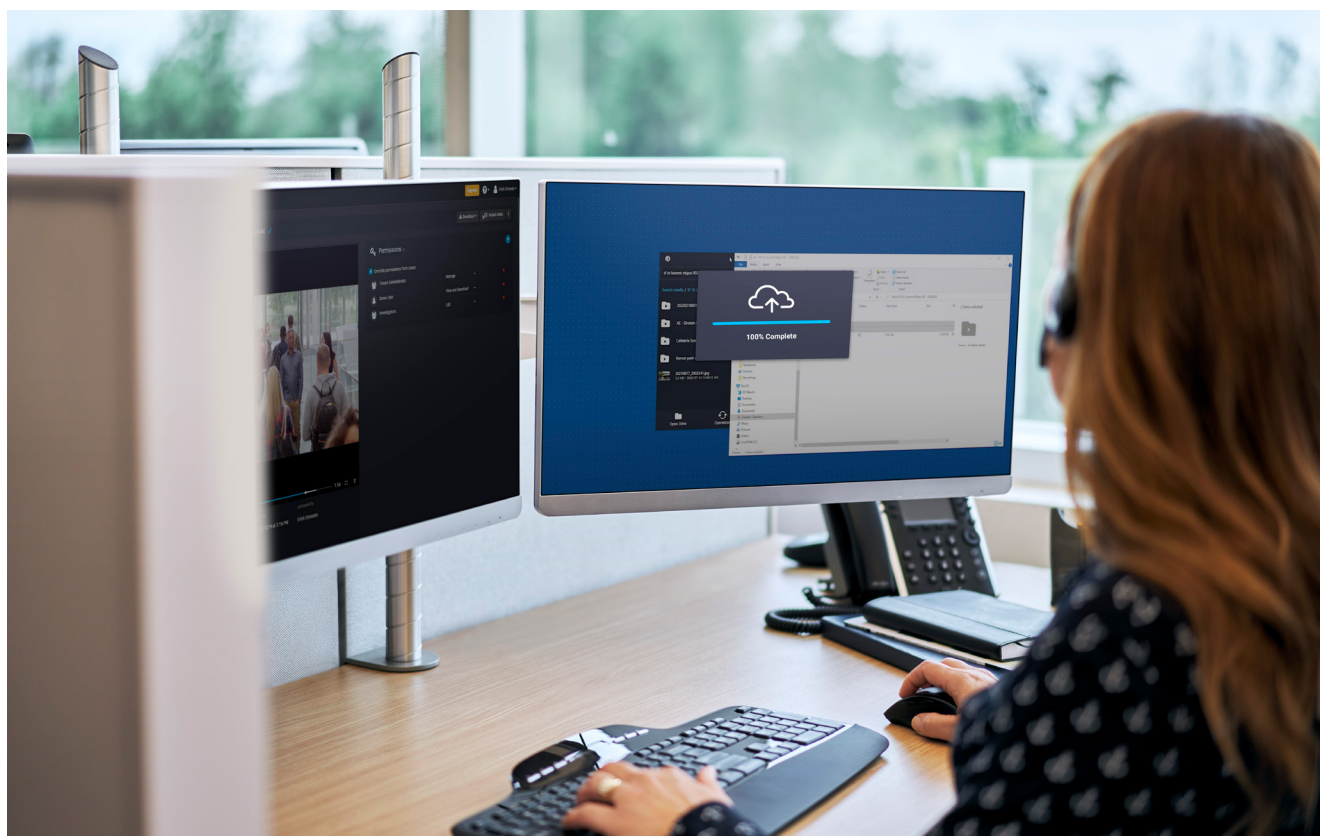
**28%**

dos usuários finais apontaram todas as soluções hospedadas na nuvem



**18%**

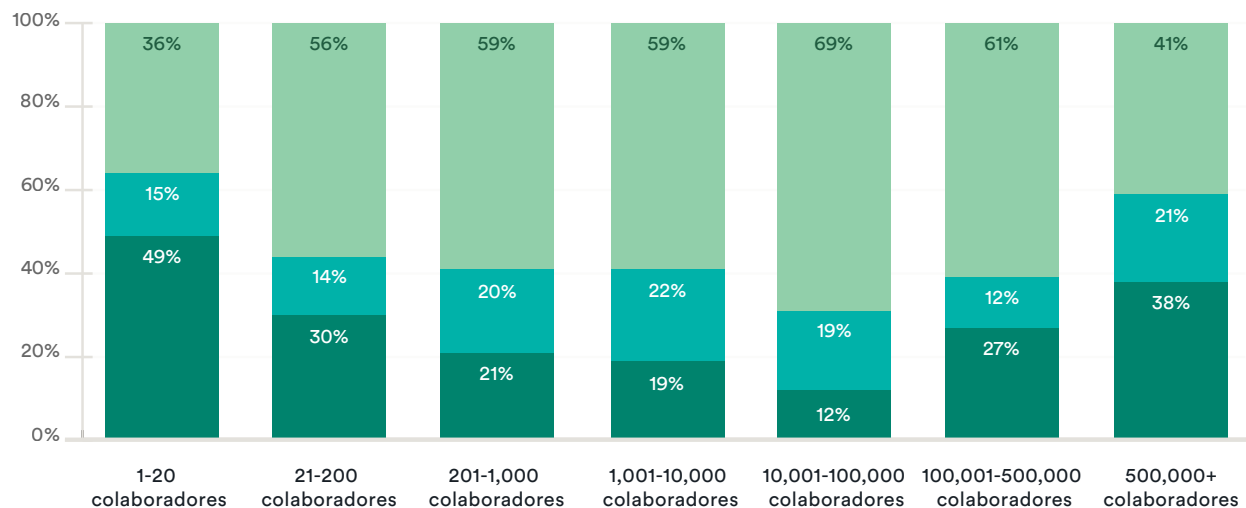
dos usuários finais apontaram nenhuma solução hospedada na nuvem





## OBSERVAÇÕES SOBRE ADOÇÃO DA NUVEM

Nos próximos 5 anos, qual é a visão-alvo da sua empresa para implantação de segurança na nuvem?



## Usuários finais entrevistados

- All cloud: todas as soluções hospedadas na nuvem
- Tudo in loco: nenhuma solução na nuvem
- Híbrido: uma combinação de soluções in loco e hospedadas na nuvem

## Cybersecurity é uma barreira

O setor de segurança física ainda fica atrás de outros setores na adoção da nuvem. A percepção da tecnologia entre os profissionais de segurança permanece conservadora. Os riscos percebidos de cybersecurity na nuvem foram classificados como o motivo mais importante para retardar a adoção da nuvem. Isso pode ser visto como uma barreira autorrealizável e baseada na falta de compreensão da cybersecurity inerente às soluções hospedadas na nuvem.

No setor de saúde, 26% dos usuários finais entrevistados indicaram que nenhuma solução seria hospedada na nuvem e no setor de governo estadual/municipal isso ficou em 24%. Embora esses setores possam estar se preparando para colocar suas ferramentas de produtividade na nuvem, parece haver resistência residual para migrar suas cargas de trabalho de segurança física para lá.

“Falta de cultura para uso da tecnologia [cloud] [na segurança física]”

– Entrevistado na pesquisa do usuário final

# Ponto de vista



A cybersecurity não precisa ser uma barreira para a adoção da nuvem. Você precisa ter controles, parceiros, procedimentos e mecanismos para gerenciar riscos. Trata-se de um modelo de responsabilidade compartilhada que pode ser altamente seguro se você fizer as escolhas certas e trabalhar com os parceiros certos.



**Mathieu Chevalier**  
Gerente e Arquiteto-Chefe de  
Segurança  
Genetec Inc.

## A segurança física e os dados relacionados são vitais

Durante as restrições da pandemia, a segurança física estava sendo usada para ajudar na movimentação segura de pessoas pelos edifícios. Isso pode contribuir para a manutenção do distanciamento social, contar pessoas e verificar se os ocupantes estão usando máscaras. No entanto, agora que as restrições da pandemia praticamente terminaram, a segurança física ainda é vista como mais do que uma ferramenta para lidar com crimes ou uma despesa necessária para manter ativos e pessoas seguras. Tornou-se um elemento central na transformação digital dos processos organizacionais.

# 63%

dos usuários finais entrevistados indicaram que a segurança física e os dados relacionados eram críticos. O resultado é semelhante à pesquisa de 2021 (68%).

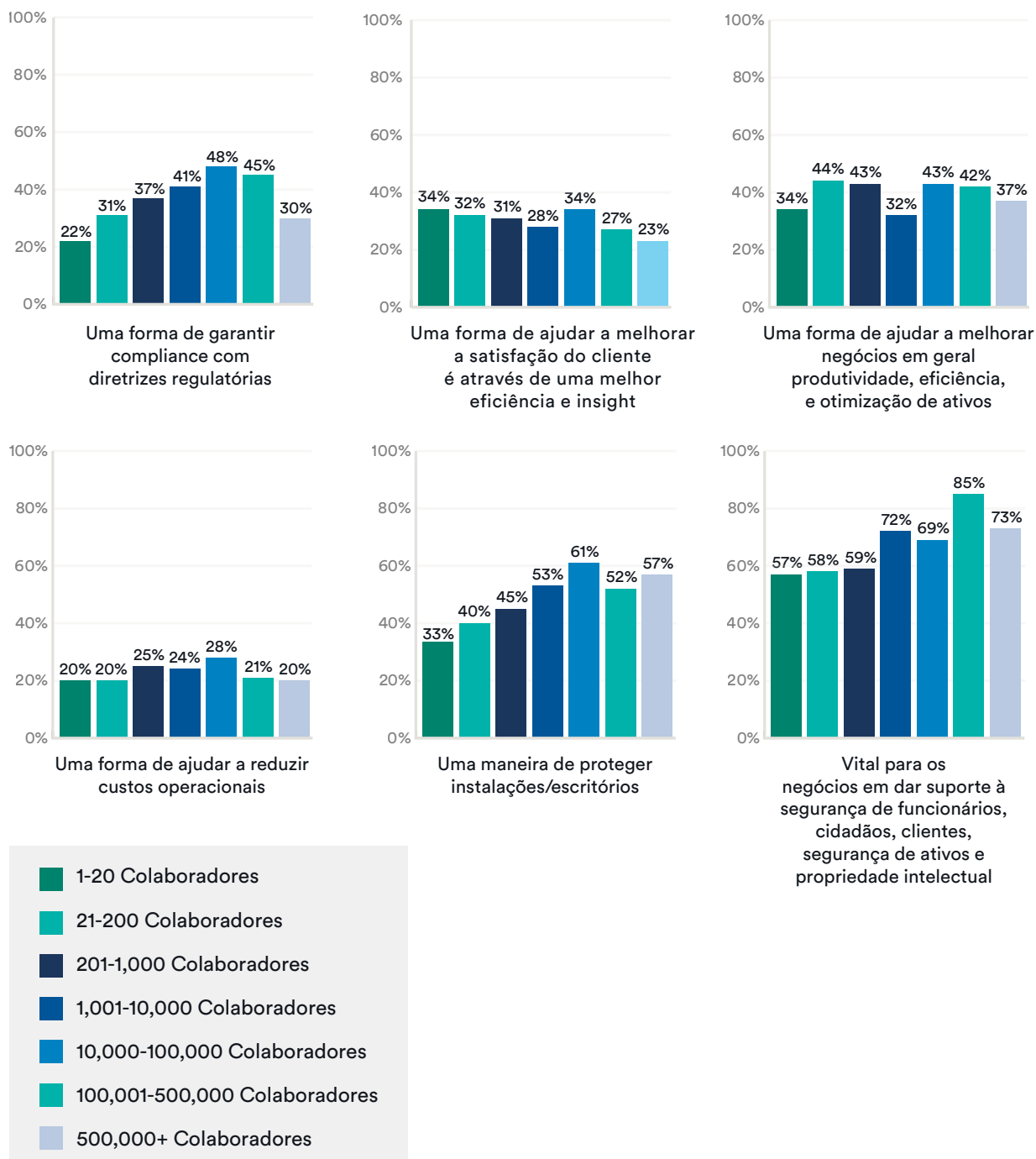
Em particular, o videomonitoramento oferece uma rica fonte de dados. As organizações podem já ter sistemas de videomonitoramento suficientes instalados, mas podem utilizar os dados existentes para alterar fundamentalmente os processos de negócios por meio da criação de novos resultados e/ou valor adicional. Os exemplos incluem o monitoramento da extensão das filas de clientes em locais de varejo ou a redução dos níveis de congestionamento nos centros das cidades, cronometrando os semáforos.

Também parece que, à medida que as organizações crescem, suas opiniões sobre o valor e/ou uso de dados de segurança física mudam. Uma porcentagem maior de usuários finais entrevistados em organizações com mais de 100.000 colaboradores indicou que a segurança física e os dados relacionados eram mais críticos do que em organizações com menos colaboradores. Isso pode ser porque estão mais avançados em suas iniciativas de transformação digital do que empresas menores. Ter gerenciamento e estrutura de dados suficientes é fundamental para agregar valor a partir dos dados coletados de sistemas de segurança físicos.

Do ponto de vista do setor do usuário final, um valor atípico notável com a maior porcentagem de entrevistados indicando que a segurança física e os dados relacionados eram essenciais, foi o setor do usuário final de transporte (71%). Aqui, a segurança física desempenha não apenas um papel crítico na segurança de colaboradores e passageiros, mas também ajuda a atender os rígidos padrões de pontualidade do trânsito.

## O PAPEL CRÍTICO DA SEGURANÇA FÍSICA

## Como as organizações veem a segurança física e dados relacionados de acordo com o tamanho da organização

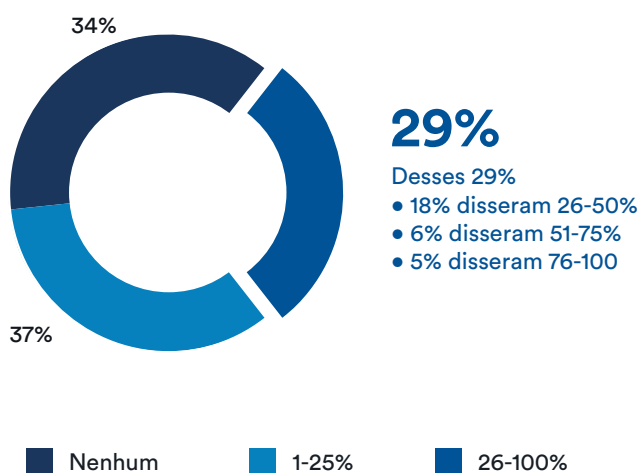


## Cybersecurity ainda é a principal prioridade

Na pesquisa de 2021, 54% dos entrevistados tinham mais de 25% de sua equipe de operações de segurança física na modalidade de trabalho remoto. Na pesquisa de 2022, caiu para 29%.

### CYBERSECURITY AINDA É A PRINCIPAL PRIORIDADE

Qual porcentagem da equipe de operações de segurança física da sua organização está na modalidade de trabalho remoto?



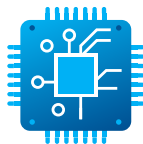
Curiosamente, 46% dos entrevistados na Europa e 48% na América Latina indicaram que nenhum de seus colaboradores de operações de segurança física foi designado para trabalhar remotamente. Isso é comparado com 21% nos EUA e Canadá e apenas 15% no Reino Unido.

À medida que as restrições pela pandemia relaxaram, o trabalho remoto diminuiu. Apesar disso, como foi o caso na pesquisa de 2021, o principal desafio enfrentado por todos os entrevistados ao gerenciar a segurança de colaboradores e visitantes continuou sendo a cybersecurity. Não é surpresa que 49% de todos os entrevistados indicaram que uma estratégia aprimorada de cybersecurity foi ativada por sua organização este ano.

Uma porcentagem maior de todos os entrevistados em organizações com mais de 100.000 funcionários indicou que o principal desafio enfrentado ao gerenciar a segurança de colaboradores e visitantes era a cybersecurity do que em organizações com menos funcionários. Isso pode ser devido ao aumento da complexidade dos sistemas de TI em organizações maiores (incluindo o número de dispositivos para proteger e gerenciar) e à percepção de que isso pode aumentar a vulnerabilidade da cybersecurity. Também pode ser devido à percepção de que organizações maiores são alvos mais atraentes para os cibercriminosos.

## CYBERSECURITY AINDA É A PRINCIPAL PRIORIDADE

## Onde os esforços de cybersecurity estão sendo focados

**40%**controle de  
acesso**39%**blindagem cibernética  
para hardware de  
segurança**37%**políticas  
de senha forte

A percepção da nuvem como um risco de cybersecurity continua sendo uma grande barreira para uma maior adoção da nuvem nas soluções de segurança física. Os entrevistados classificaram esses riscos percebidos como o fator mais importante para desacelerar a adoção de soluções hospedadas na nuvem para aplicações de segurança física. Da mesma forma, os usuários finais classificaram esses riscos percebidos como o fator mais importante para dissuadir sua organização de implantar sistemas de segurança na nuvem. Apesar disso, conforme mostrado anteriormente neste relatório, a transição gradual da segurança física para a nuvem continua.



## A segurança física torna-se unificada

Para alguns, as restrições da pandemia atuaram como um catalisador adicional para unificar seus sistemas de videomonitoramento e controle de acesso, pois alguns usuários finais precisavam dar esse passo para gerenciar com eficácia o movimento seguro dos ocupantes em suas instalações. A crescente demanda por essa abordagem pode ter feito com que alguns integradores de sistemas ganhassem maior experiência e consciência dos benefícios da unificação, resultando em mais recomendações para os usuários finais considerarem essa abordagem.

De acordo com as respostas da pesquisa, regionalmente, os usuários finais dos EUA e do Canadá foram os que mais provavelmente implantaram um sistema unificado de controle de acesso e vídeo (onde o software de controle de acesso e vídeo são unificados como um sistema de um único fabricante).

44,4% dos entrevistados nos EUA e no Canadá disseram que implantaram um sistema unificado de controle de acesso e vídeo, uma porcentagem maior do que em todas as outras regiões.



possuem videomonitoramento e controle de acesso em suas implantações de segurança física.



**Desses 64%, mais de 75% possuem:**

- integração entre sistemas de videomonitoramento e controle de acesso de diferentes fornecedores, ou
- Unificação de soluções de videomonitoramento e controle de acesso de um único fabricante



## Mudanças na tecnologia – o ano passado

Na fase inicial da pandemia, o interesse cresceu rapidamente por uma variedade de soluções de segurança que poderiam ajudar no gerenciamento de visitantes, implementar regulamentações governamentais e melhorar os recursos remotos. O interesse por algumas dessas soluções diminuiu em 2021 e a pesquisa mais recente sugere que caiu ainda mais em 2022.

Uma porcentagem menor de todos os entrevistados na pesquisa de 2022 indicou que as capacidades associadas à pandemia eram uma prioridade. A pesquisa de 2022 também indicou que os recursos “tradicionais relacionados à segurança” eram o foco.



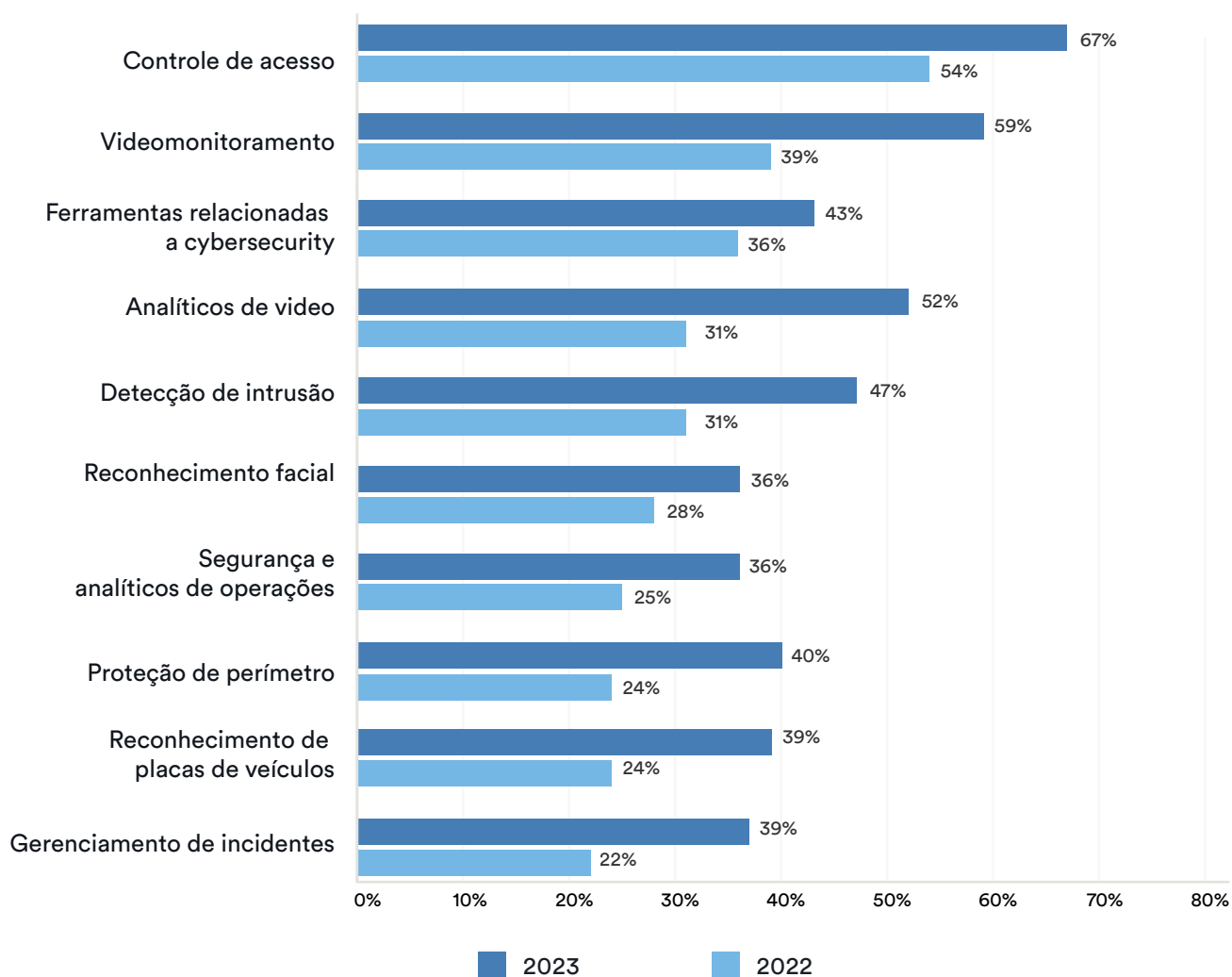
## Mudanças na tecnologia – o ano à frente

Conforme mencionado anteriormente neste relatório, a unificação entre controle de acesso e videomonitoramento aumentou em importância para muitas organizações. O trabalho que foi deixado de lado para os sistemas principais durante a pandemia, agora está sendo repriorizado. O controle de acesso e videomonitoramento são dois sistemas, entre outros, que estão centralizando os esforços no trabalho do sistema principal para 2023.



## MUDANÇAS NA TECNOLOGIA - O ANO PASSADO VERSUS O PRÓXIMO ANO

## As 10 principais tecnologias em que as organizações planejam investir



# Principais aprendizados



## 1 A economia e supply chain são desafios que podem ser superados

As restrições da pandemia começaram a diminuir gradualmente na maioria dos países em 2021 e 2022, mas deixaram reais efeitos colaterais. Esses efeitos econômicos estão afetando o setor de segurança física na forma de escassez de produtos e dificuldades com RH. Esses fatores também estiveram presentes em 2022, e as previsões para 2023 são incertas, tornando isso uma preocupação constante para as empresas. Apesar dos efeitos dos problemas contínuos com a mudança de oferta, economia e previsões de recessão, a pesquisa aponta para um sinal otimista de uma perspectiva geral positiva para os investimentos OPEX de 2023.

## 2 Priorizando a segurança dos sistemas de segurança física

Embora o setor de segurança física esteja atrasado em seu foco em cybersecurity comparado a outros setores, é evidente que ocorreu uma mudança e que a necessidade de priorizar essas iniciativas como parte do gerenciamento do sistema de segurança física também aconteceu. O principal desafio enfrentado no gerenciamento da segurança de colaboradores e visitantes continuou sendo a cybersecurity em 2022. Essa também é uma das principais prioridades para 2023.

## 3 A migração para a nuvem continua

Embora o setor de segurança física ainda esteja atrás de outros setores na adoção da nuvem, há sinais claros de que o movimento nessa direção continuará. Tudo indica que as implantações de nuvem híbrida são o caminho a seguir para as empresas, para que possam racionalizar seus custos, preocupações e abordagem para migrar para a nuvem.

# 31%

de todos os entrevistados disseram que os orçamentos devem aumentar para 2023

# 34%

de todos os entrevistados disseram que os orçamentos devem permanecer estáveis para 2023

# 16%

de todos os entrevistados disseram que os orçamentos devem cair para 2023

# 36%

dos entrevistados desejam investir em ferramentas relacionadas à cybersecurity para melhorar seu ambiente de segurança física nos próximos 12 meses

# 66%

de todos os entrevistados indicaram que, durante os próximos dois anos, sua organização passará a gerenciar ou armazenar mais dados de segurança física na nuvem

# Ponto de vista



Os provedores de serviços compartilhados dentro dos usuários finais estão descobrindo que precisam aprimorar suas habilidades para lidar com:

- Crescente envolvimento de outros stakeholders nos negócios que têm interesse nos dados subjacentes
- Superando as preocupações com a cybersecurity e o uso responsável da rede
- Equilibrar o interesse entre aproveitar os avanços tecnológicos e restrições internas, como financiamento e escassez de talentos



**Pervez Siddiqui**  
Vice-presidente de Ofertas e  
Transformação  
Genetec Inc.

# Apêndice



## Apêndice 1 - Metodologia de pesquisa

A Genetec Inc. entrevistou profissionais de segurança física de 24 de agosto a 21 de setembro de 2022.

O objetivo da pesquisa foi:

- obter uma visão das operações e ambientes de segurança física
- entender a resposta das organizações a desafios externos, como escassez de produtos e dificuldades com RH
- entender o foco global para 2023

Após uma revisão das entrevistas e filtragem de dados, 3.711 entrevistados foram incluídos na amostra para análise.

### Detalhes sobre a pesquisa e análise

- O público-alvo da pesquisa focou em indivíduos que trabalham para organizações que participam de compras, gerenciamento, serviços e/ou uso de tecnologia de segurança física. O público-alvo incluiu usuários finais da Genetec, bem como participantes alcançados por meio de publicidade digital ou contatados diretamente por terceiros por meio de suas listas de e-mail opt-in.
- Convites para participar da pesquisa on-line foram enviados a participantes em potencial por e-mail em inglês, francês, alemão, holandês, italiano, espanhol, português, japonês e coreano.
- O formulário de pesquisa online estava disponível em inglês, francês, alemão, holandês, italiano, espanhol, português, japonês e coreano.
- Somente pesquisas totalmente preenchidas e enviadas por indivíduos dentro do público-alvo do estudo foram incluídas na análise final.
- As amostras da pesquisa foram realizadas em todas as regiões, incluindo EUA e Canadá, México, América Central, Caribe, América do Sul, Europa, Oriente Médio, África, Leste Asiático, Sul da Ásia, Sudeste Asiático, Ásia Central, Ásia Ocidental e Austrália/Nova Zelândia.
- As taxas de resposta e de conclusão da pesquisa variaram de acordo com a região e o tamanho da organização, potencialmente introduzindo erros de amostragem em conjuntos de subamostras.
- As respostas foram coletadas de dois públicos-alvo principais: usuários finais de segurança física e integradores de sistemas. A filtragem de dados foi realizada para validar a classificação do entrevistado em um desses dois públicos e limitar possíveis erros. Considera-se que quaisquer erros não amostrais resultam da coleta de dados fora do público-alvo (por exemplo, indivíduos que se identificam incorretamente como usuários finais quando, na verdade, são contratados por integradores de sistemas).

### Uma observação sobre os cálculos da pesquisa:

Devido ao arredondamento e ao modelo da pesquisa (incluindo escala de classificação, marque todas as que se aplicam e questões de múltipla escolha), nem todos os percentuais totais neste relatório serão iguais a 100%. Para todas as perguntas aplicáveis (onde os entrevistados podem escolher várias respostas), as porcentagens referem-se à proporção de entrevistados que escolheram a resposta individual.

## Apêndice 2 - Informações demográficas da pesquisa

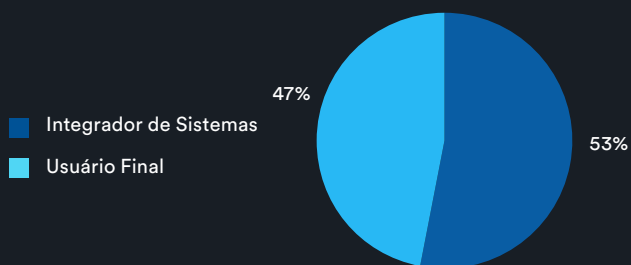
### INDÚSTRIAS

Serviços de Sistemas de Segurança	55%
Outros	8%
Educação	6%
Transporte	5%
Bancário e Finanças	3%
Energia e serviços de utilidade pública	3%
Segurança Nacional	2%
Engenharia e Construção	2%
Manufatura e Atacado	2%
Tecnologia e Mídia	2%
Saúde	2%
Varejo	2%
Administração Pública	2%
Alimentos, Cosméticos, Produtos Químicos e Farmacêuticos	2%
Transporte e Logística	1%
Gestão de Propriedade	1%
Serviços Profissionais e Associações	1%
Jogos	1%

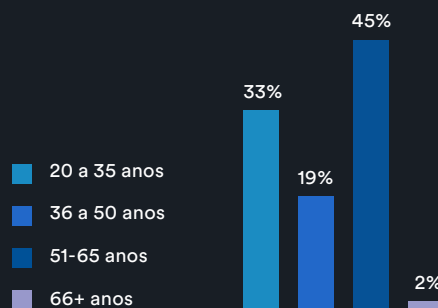
### FUNÇÃO NO TRABALHO

Engenharia, R&D, Projeto de Sistema e Garantia de Qualidade	23%
Gerenciamento de Instalações/Operações	14%
Vendas	11%
Tecnologia da Informação (TI)	10%
Serviço ao Cliente ou Suporte (Incluindo Suporte Técnico)	8%
Gerenciamento de Projetos/Risco ou Gerenciamento de Compliance	8%
Administração/Administração de Escritórios	6%
Segurança e Proteção	5%
Contabilidade/Finanças	3%
Administração, Jurídico	3%
Estimativa	2%
Marketing	2%
Jurídico	1%
Compras e Suprimentos	1%
Gestão da Qualidade	1%

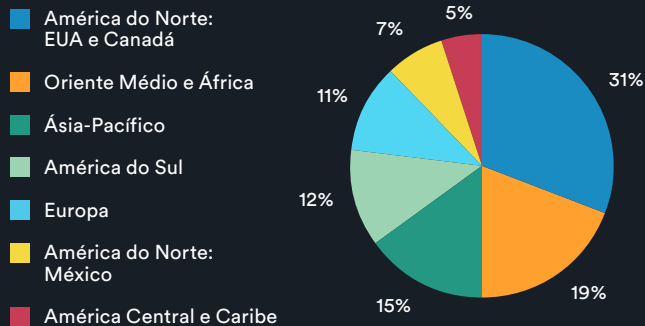
### TIPO DE ENTREVISTADO



### FAIXA ETÁRIA DO ENTREVISTADO



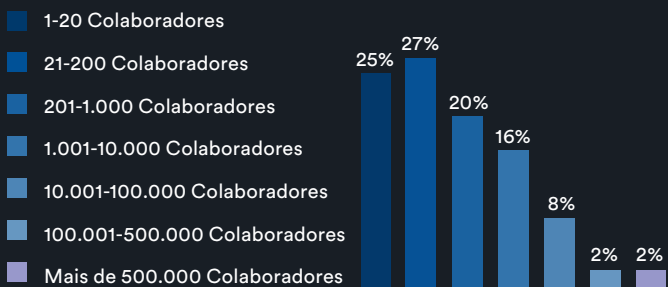
## REGIÕES GEOGRÁFICAS



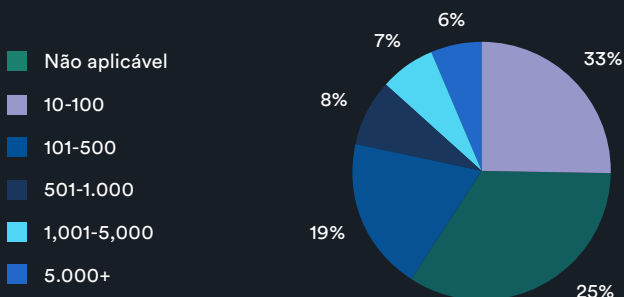
## RECEITA ORGANIZACIONAL (USD)

USD 5M a 24,9M	31%
USD 25M a 199,9M	16%
USD 200M - USD 499,9M	11%
USD 500M a 999,9M	6%
USD 1B-10B	4%
USD 10B +	2%
Não foi possível divulgar	30%

## CONTAGEM GLOBAL DE COLABORADORES DA ORGANIZAÇÃO

DEPARTAMENTO DE SEGURANÇA FÍSICA  
CONTAGEM DE COLABORADORES

1-20 Colaboradores	54%
21-200 Colaboradores	29%
201-1.000 Colaboradores	11%
1.001-10.000 Colaboradores	5%
Mais de 10.000 Colaboradores	2%

IMPLANTAÇÃO DE VIDEOMONITORAMENTO  
(# DE CÂMERAS)IMPLANTAÇÃO DE CONTROLE DE ACESSO  
(# DE CRACHÁS OU LEITORES DE ACESSO SEM CONTATO)

Não aplicável	36%
1 - 20	13%
21 - 200	13%
201 - 1.000	14%
1.001 - 5.000	10%
5.001 +	14%

## Apêndice 3 - Comentários abertos

Os participantes da pesquisa puderam fornecer comentários adicionais associados a algumas perguntas da pesquisa. A seguir estão as respostas selecionadas que são representativas dos sentimentos gerais:

### **Sua organização implanta outros tipos de infraestrutura de segurança física?**

- Alarmes
- Áudio
- Barreiras automatizadas
- Estacionamento com controle automatizado
- Biometria
- Mourões
- Cancelas
- Sistemas de gerenciamento de edifícios
- Drones
- Cercas elétricas
- Sistema de Alerta de Emergência (EAS)
- Detectores de explosivos
- Reconhecimento por impressão digital
- Sistemas de detecção e controle de incêndios
- Luzes de inundação
- Lidar
- Scanners de bagagem
- Detectores de metal
- Rádios móveis
- Radar
- Sistema de localização em tempo real
- Monitoramento de ativos RFID
- Catracas
- Sistemas de raios X

### **Houve algum outro motivo que levou sua organização a começar a usar a nuvem para aplicações de segurança física?**

- Capacidade de unificar produtos e compartilhar feeds do sistema com Parceiros CI/Aplicação da lei
- O armazenamento na nuvem é mais seguro e conveniente
- Compliance com regulamentações governamentais
- Segurança de dados
- Obtenha certificação de segurança de acordo com as diretrizes de segurança nacional
- Fácil de usar

- Temor de roubo NVR
- Evite a perda de dados gravados se o hardware for roubado
- Redundância/backup de gravação
- Redução da equipe /salários para TI
- Regulamentações do setor
- Falta de profissionais de TI
- Pequeno Capex necessário
- Velocidade de acesso aos arquivos

### **Alguma outra coisa retardou a adoção de soluções hospedadas na nuvem por parte de sua organização para aplicações de segurança física?**

- Acesso a banda larga suficiente
- Os dados armazenados na nuvem não pertencem mais a você, é preciso um administrador de dados para usá-los
- Problemas de conectividade
- RGPD
- Falta de cultura voltada ao uso da tecnologia
- Quedas de energia

### **Existem outras razões que dissuadiram sua organização de implantar soluções de segurança na nuvem?**

- RGPD
- Falta de espaço suficiente em nosso data center
- Proibição para Infraestrutura Crítica

### **Que tipo de projetos serão o foco do seu departamento para o próximo ano?**

- Drones
- Vigilância Eletrônica de Artigos
- Detecção e controle de incêndios
- Gerenciamento e monitoramento de ativos IoT
- Controle de estoque logístico
- Botões de pânico
- Integrações de terceiros que proporcionam menos consumo de energia
- Violação de trânsito

**Selecione os 3 principais desafios enfrentados pela sua organização em 2022**

- Restrições orçamentárias
- Mudanças nas políticas governamentais
- Prazos de entrega demorados
- Falta de materiais
- Consumo de energia
- Regulamentações
- Aumento de custos

**Que tipo de desafios de RH afetaram seu departamento de segurança física no último ano?**

- Constante rotatividade/redesignação de pessoal
- Altas taxas de inflação e salários elevados
- Falta de orçamento para treinamento

**Quais novos processos ou prioridades foram ativados pela sua organização este ano?**

- Desenvolvimento de aplicações
- Mudança de CRM/ERP
- Sistema de segurança contra incêndio
- Redução de emissões até 2025
- Trabalho remoto

**Quais capacidades você priorizou no ano passado?**

- Controle de acesso
- Cybersecurity
- Reconhecimento facial
- Detecção e controle de incêndios
- PSIM
- Analíticos de vídeo
- Monitoramento da vida selvagem por GPS

**Que tipo de projetos foram afetados? (por atrasos causados devido a problemas na supply chain)**

- Novas instalações/projetos
- Mudanças de escritório

**Como você respondeu a atrasos causados por problemas na supply chain?**

- Equipamento alugado de um subcontratado
- Inventário aumentado
- Comprado anteriormente

**Quais dos seguintes recursos de cybersecurity e proteção de dados você implementou recentemente no último ano?**

- Auditorias do sistema de informação
- Certificação ISO27K
- VLAN isolada para dispositivos de segurança IOT
- Planos contingentes operacionais
- Somente comunicações de saída
- VPN
- Lista de permissões de endereços IP específicos e portas de comunicação

**Existem outros recursos remotos frequentemente solicitados por seus clientes?**

- Monitoramento de controle de acesso
- Acesso a mapas baseados em GIS
- Ativar e desativar
- Alertas para plataformas de mensagens como Telegram, Signal ou Whatsapp
- Gestão de casos
- Privacidade de dados
- Diagnóstico e integridade do sistema
- Sistemas Eletrônicos de Proteção de Ativos (EAS)
- Geolocalização
- Sistema de monitoramento de rondas
- Controle de integração HVAC ao sistema de segurança
- Integração com sistemas de alarme de incêndio
- Intercomunicadores
- Compartilhamento de vídeo ao vivo para terceiros
- Controle de rotas logísticas
- Chamada para enfermeiros
- Botões de pânico
- Manutenção preventiva
- Comunicação de áudio remota
- Manutenção remota
- Gerenciamento de sistemas de terceiros
- Controle remoto UAV
- Virtualização



**Em quais soluções seus clientes desejam investir para evoluir ou melhorar as implantações de segurança física nos próximos 12 meses?**

- Sistema de Alerta de Emergência (EAS)
- Sistemas de detecção e controle de incêndios
- Botões de pânico
- Contagem de pessoas
- Tecnologia de detecção de objetos usando ondas de rádio para determinar o intervalo, altitude, direção e velocidade de tais objetos
- Detecção térmica
- Monitoramento da vida selvagem por GPS

**Quais ações você executou para mitigar os problemas de aquisição e inventário de hardware relacionados aos atuais desafios da supply chain?**

- Permitir que os clientes façam pedidos antecipados antes do lançamento do concurso
- Certos projetos são simplesmente adiados se não houver substituto
- Direcionar esforços para serviços profissionais e suporte técnico
- Prazos de entrega demorados
- Abriu um centro de reparos para trazer de volta para a produção alguns eletrônicos fáceis de consertar
- Sistemas de re-design
- Use equipamentos de segunda mão

**Outras operações serão afetadas pelo trabalho em sua carteira de implantação?**

- Acesso a financiamento
- Todas as operações serão afetadas
- Fluxo de caixa, faturamento, coleta de receita
- Cuidados de cybersecurity para trabalho remoto
- Eletricidade e outros serviços de fornecimento
- Segurança ambiental
- Tudo está conectado
- Recursos Humanos
- Logística
- Contratos de manutenção
- Fabricação
- Operações
- Disponibilidade de equipe qualificada
- O treinamento para novas marcas que incorporamos ao portfólio de soluções foi adiado



## Sobre a Genetec

A Genetec Inc. é uma inovadora empresa de tecnologia com um amplo portfólio de soluções que abrange segurança, inteligência e operações. O produto carro-chefe da empresa, Security Center, é uma plataforma de segurança física que unifica videomonitoramento IP, controle de acesso, reconhecimento automático de placas de veículos (ALPR), comunicações e analíticos. A Genetec também desenvolve soluções hospedadas na nuvem e serviços projetados para melhorar a segurança e contribuir com novos níveis de inteligência operacional para governos, empresas, transporte e as comunidades em que vivemos. Fundada em 1997 e com sede em Montreal, Qc, Canadá, a Genetec atende seus clientes globais por meio de uma ampla rede de revendedores, integradores, parceiros de canal certificados e consultores em mais de 159 países.

Para saber mais sobre nós, acesse  
**[genetec.com/br](https://www.genetec.com/br)**

Para mais informações sobre este relatório,  
por favor entre em contato **[Genetec-research@genetec.com](mailto:Genetec-research@genetec.com)**

**Genetec Inc.**  
[genetec.com/br/fale-conosco](https://www.genetec.com/br/fale-conosco)  
[info@genetec.com](mailto:info@genetec.com)  
[@genetec](https://www.genetec.com/br)

© Genetec Inc., 2022. Genetec e o Logo Genetec são marcas comerciais da Genetec Inc., e podem estar registradas ou pendentes de registro em diversas jurisdições. Outras marcas registradas usadas neste documento podem ser marcas registradas dos fabricantes ou fornecedores dos respectivos produtos.