RELATÓRIO

# Relatório sobre a situação da tecnologia operacional e da segurança cibernética 2022

# ÍNDICE

# Infográfico: principais descobertas

## Pessoas

**33%** das organizações confiam a segurança de redes industriais ao VP/ diretor de operações/ engenharia de rede

**67%** dos líderes de segurança de redes industriais vêm de uma formação em engenharia de TO

**43%** dos participantes consideram o tempo de resposta a incidentes de segurança um dos três principais métricas do sucesso

## Postura de segurança


**56%** das organizações informam estar no nível 3 ou 4 de maturidade da segurança de redes industriais


**50%** dizem que a postura de segurança de redes industriais é um fator significativo na pontuação global de risco

**13%** das organizações têm visibilidade centralizada de todas as atividades de TO

## Práticas de segurança

**48%** informam comprometimentos de segurança à gerência executiva

**32%** implementaram um controle de acesso à rede com base na função

**52%** dizem que todas as atividades de TO são monitoradas e seguidas pelo SOC

## Resultados da segurança

**93%** das organizações tiveram mais de 1 invasão no ano passado **78%** tiveram mais de 3

**61%** das invasões impactaram os sistemas de TO

**90%** das invasões demandaram horas ou mais até que o serviço fosse restaurado

## Melhores práticas

### As organizações de alto nível são mais propensas a

- Ter uma visibilidade centralizada
- Ser avaliadas pelo tempo de resposta à vulnerabilidade
- Implementar NAC com base na função
- Informar comprometimentos de segurança
- Usar um único fornecedor de dispositivos de TO

# Resumo executivo

O Relatório sobre o estado da tecnologia operacional e da segurança cibernética de 2022, agora em sua quarta edição anual, constata que as organizações continuam avançando muito lentamente rumo à proteção total de seus ativos de tecnologia operacional (TO). Isto ocorre em um momento em que os sistemas de TO estão se tornando mais importantes para o bem-estar de muitas organizações, os eventos geopolíticos aumentam a probabilidade de ataques, mais sistemas de TO estão sendo conectados à internet e as ameaças baseadas em IP estão se tornando mais avançadas e causando mais danos. Esta combinação de fatores aumenta a necessidade da segurança de redes industriais na carteira de risco de muitas organizações.

Com base em uma pesquisa global com mais de 500 profissionais de segurança de redes industriais, o relatório deste ano constata que, embora a segurança de redes industriais tenha a atenção dos líderes organizacionais, continua sendo assunto de profissionais de hierarquia relativamente inferior. A especulação de que a segurança de redes industriais será acrescida às funções do CISO tem estado em voga há anos, mas não há sinais de que as coisas estejam avançando nessa direção. E, embora a segurança seja uma parte das métricas de desempenho para a maioria dos participantes, muitos são avaliados mais com relação a fatores de eficiência, o que pode levar ao cortar de gastos com segurança.

**Com base em uma pesquisa global com mais de 500 profissionais de segurança de redes industriais, o relatório deste ano constata que, embora a segurança de redes industriais tenha a atenção dos líderes organizacionais, continua a ser assunto de profissionais de hierarquia relativamente inferior.**

As organizações demonstram avanços modestos na maturidade global de sua postura de segurança de redes industriais, com mais algumas poucas avançando para o nível 3. Mas a análise das melhores práticas específicas traz nuances à questão. Apenas 13% dos participantes conseguiram uma visibilidade centralizada de todas as atividades de TO, e apenas 52% são capazes de acompanhar todas as atividades de TO a partir do centro de operações de segurança (SOC). Apenas cerca de metade dos participantes afirma rastrear e informar várias métricas básicas de segurança, e menos de metade está utilizando qualquer uma das dezenas de tecnologias e práticas específicas de segurança. Esta última resposta indica uma diversidade na forma como as organizações abordam a segurança de redes industriais, e reflete um mercado que ainda está em evolução.

Algo que melhorou muito pouco no último ano foram os resultados de segurança das organizações. 93% das organizações sofreram uma invasão nos últimos 12 meses, e 78% experimentaram mais de três. Os impactos incluíram tempo de inatividade, perda financeira ou de dados, rebaixamento da marca e até mesmo redução da segurança física. Claramente, a maioria das organizações tem muito trabalho a fazer. Felizmente, uma pequena porcentagem dos participantes conseguiu evitar invasões no último ano, e este relatório identifica várias das melhores práticas que eles empregaram com mais frequência.

# Introdução

Embora a TO seja menos visível do que a TI na maioria das organizações — e, certamente, no imaginário público —, não é menos importante para a economia e para a vida quotidiana das pessoas. Afinal, os sistemas de TO controlam as infraestruturas críticas de que todos dependem — a rede elétrica, os sistemas de água e esgoto, os oleodutos de combustível, centrais elétricas e redes de transporte. E é essencial para a fabricação de todos os tipos de bens.

A TO é uma componente importante da transformação digital nas organizações industriais. A rápida evolução das condições de mercado tornou a adoção de metodologias e tecnologias da "Indústria 4.0" praticamente essencial, mesmo antes da COVID-19. A pandemia apenas acelerou tais tendências, deixando os "inimigos" da tecnologia confusos tentando atualizar e aperfeiçoar suas operações.[1]

## Ameaças crescentes de segurança

Esta tendência não escapou à atenção dos criminosos. No ano passado, o Relatório de cenário de ameaças global, dos FortiGuard Labs, observou um aumento significativo nas detecções de sistemas de prevenção de intrusão (IPS) em sistemas de TO.[2] Esta observação coincidiu com vários eventos de segurança de alto nível que afetaram os sistemas de TO, incluindo ataques de ransomware à Colonial Pipeline e à JBS, que perturbaram o fornecimento de gasolina e carne na América do Norte em maio e junho passados.[3]

Uma razão para o aumento dos ataques cibernéticos a sistemas de TO na última década é que eles se tornaram mais vulneráveis a ataques de fora. Enquanto os sistemas de TO eram tradicionalmente isolados dos sistemas de TI, estas duas infraestruturas estão, hoje, quase universalmente integradas. Isso significa que os sistemas de TO estão agora conectados à internet e, teoricamente, podem ser acessados de qualquer lugar. Isto, em si, representa um aumento significativo da superfície de ataque das organizações industriais, e a crescente ubiquidade dos dispositivos da Internet das Coisas Industrial (IIoT) alarga ainda mais essa superfície de ataque. Ao mesmo tempo, os sistemas de TO conectados estão vulneráveis a um cenário de ameaças de TI que está se tornando cada vez mais avançado.

A invasão russa da Ucrânia e eventos relacionados colocaram outro foco de atenção na segurança de redes industriais. Em abril de 2022, a Agência de Segurança Cibernética e Infraestruturas dos EUA (CISA), juntamente com seus homólogos na Austrália, Canadá, Nova Zelândia e Reino Unido, advertiram que criminosos patrocinados pelo Estado russo intensificaram seus esforços em resposta às sanções prejudiciais impostas pelo Ocidente. As agências exortam os responsáveis por redes de infraestruturas críticas a "se prepararem e reduzirem potenciais ameaças cibernéticas — incluindo malware destrutivo, ransomware, ataques DDoS e espionagem cibernética — por meio do fortalecimento de suas defesas cibernéticas e da realização de diligência prévia de indicadores de atividade maliciosa."[4]

De fato, houve um aumento de ataques atribuídos à Rússia, e as organizações ucranianas suportaram as consequências.[5] Mas as organizações no resto do mundo são tudo menos imunes, com sete em cada dez fornecedores de infraestruturas nacionais críticas (CNI) no Reino Unido tendo informado um aumento de ataques cibernéticos desde o início da guerra.[6]

## Um ponto focal crescente na segurança de redes industriais

O resultado é que as empresas em muitos setores estão se esforçando para oferecer segurança a sistemas de TO cada vez mais vulneráveis. A investigação da Westlands Advisory[7] para a Fortinet concluiu que o investimento em tecnologias de segurança de TI/TO e de TO específicas totalizou 6,9 bilhões de dólares para todo o ano de 2022. E tais investimentos estão aumentando mais rapidamente do que os gastos com TI apenas, com uma taxa de crescimento anual composta (CAGR) projetada de 21% para segurança de redes industriais e de 16% para segurança cibernética de TO/TI entre agora e 2027.

Embora este investimento crescente seja um sinal muito bom, o relatório conclui que, de um modo geral, as organizações representadas na pesquisa deste ano ainda têm uma distância considerável a percorrer para protegerem adequadamente seus sistemas de TO. Mas um pequeno subconjunto de participantes conseguiu atravessar os últimos 12 meses sem sofrer uma invasão sequer, e o relatório tenta destacar algumas das coisas que tais organizações fizeram direito.

# Metodologia para este estudo

O Relatório sobre o estado da tecnologia operacional e da segurança cibernética deste ano se baseia em uma pesquisa com mais de 500 profissionais de TO, realizada entre 14 e 18 de março de 2022. As perguntas da pesquisa refletem, em grande parte, as feitas em pesquisas semelhantes em 2019, 2020 e 2021, retratadas em versões anteriores deste relatório. Os participantes preencheram 40 questões sobre o estado de suas infraestruturas de TO e segurança de redes industriais, melhores práticas de segurança e o processo de seleção de fornecedores.

## Regiões, cargos, setores e dispositivos diferentes

Uma diferença na amostragem da pesquisa deste ano em relação aos anos anteriores é que ela é de natureza global e não restrita apenas ao universo norte-americano (Figura 1). No total, os participantes vêm de um total de 28 países, com 150 participantes baseados na América do Norte (NA); 70 na América Latina (LATAM); 130 na Europa, Médio Oriente e África (EMEA); e 170 na Ásia e Pacífico (APAC).

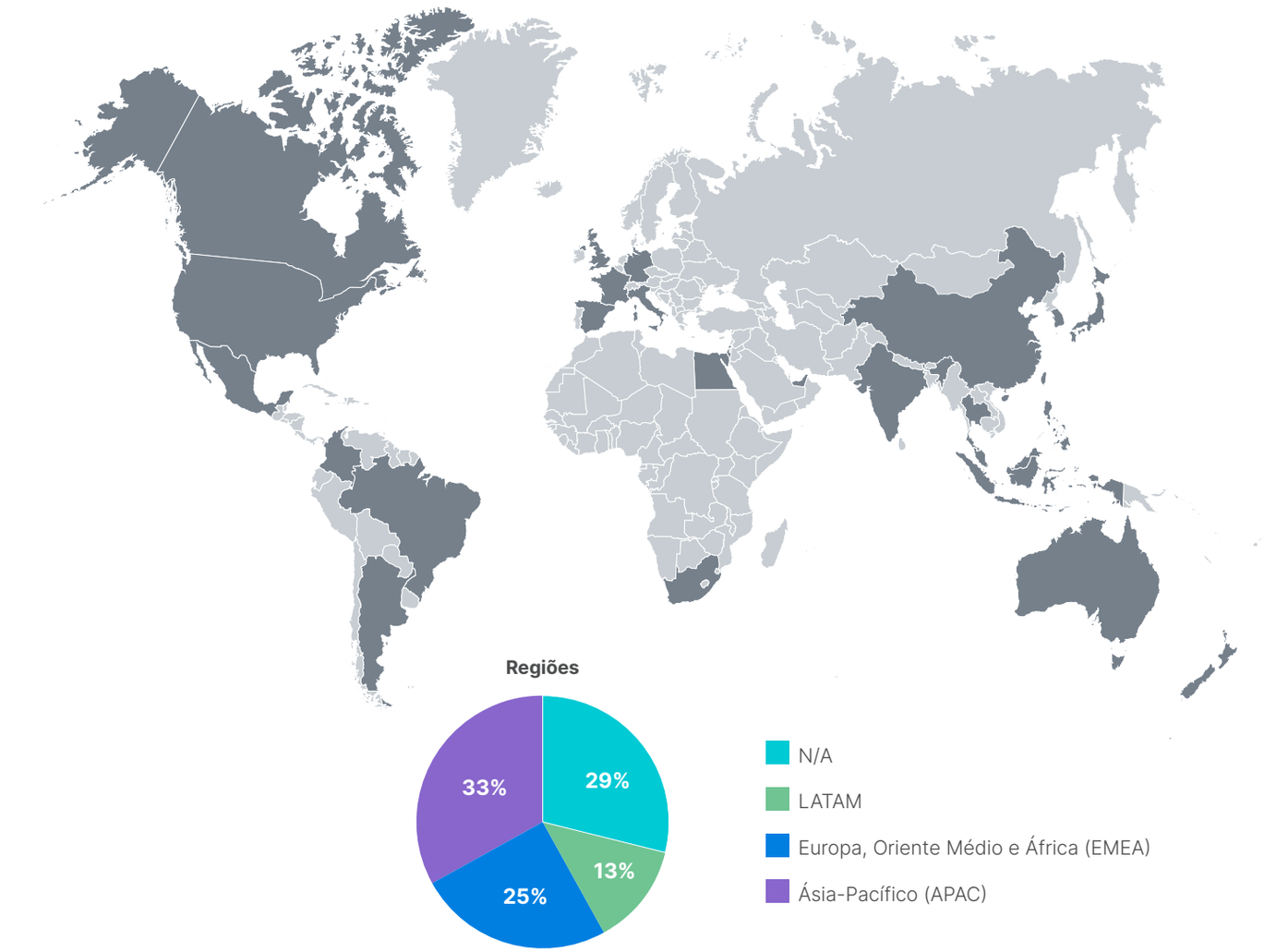



Figura 1: Países e regiões representados na pesquisa.

A pesquisa buscou pessoas em cargos de liderança, responsáveis pela TO e a segurança de redes industriais, desde gerentes até executivos de nível C (Figura 2). Representam uma gama de setores que são grandes usuários de TO, incluindo fabricação, transporte e logística, além de cuidados de saúde. Seis em cada 10 participantes são os responsáveis finais pela tomada de decisões quando se trata da compra de TO, e 85% dizem ser consultados periodicamente sobre compras de segurança cibernética (Figura 3).

Os participantes são usuários do sistema de controle industrial (ICS) e de Supervisory Control and Data Acquisition (SCADA) fabricados por 15 fornecedores diferentes (Figura 4). Assim como em anos anteriores, a Honeywell e a Siemens continuam sendo as marcas mais comuns em uso pelos participantes, com mais usuários da Honeywell e Schneider do que em anos anteriores. A utilização da Siemens e da Yokogawa diminuiu significativamente durante o mesmo período. Algumas destas alterações refletem a amostragem geográfica mais ampla na pesquisa deste ano.

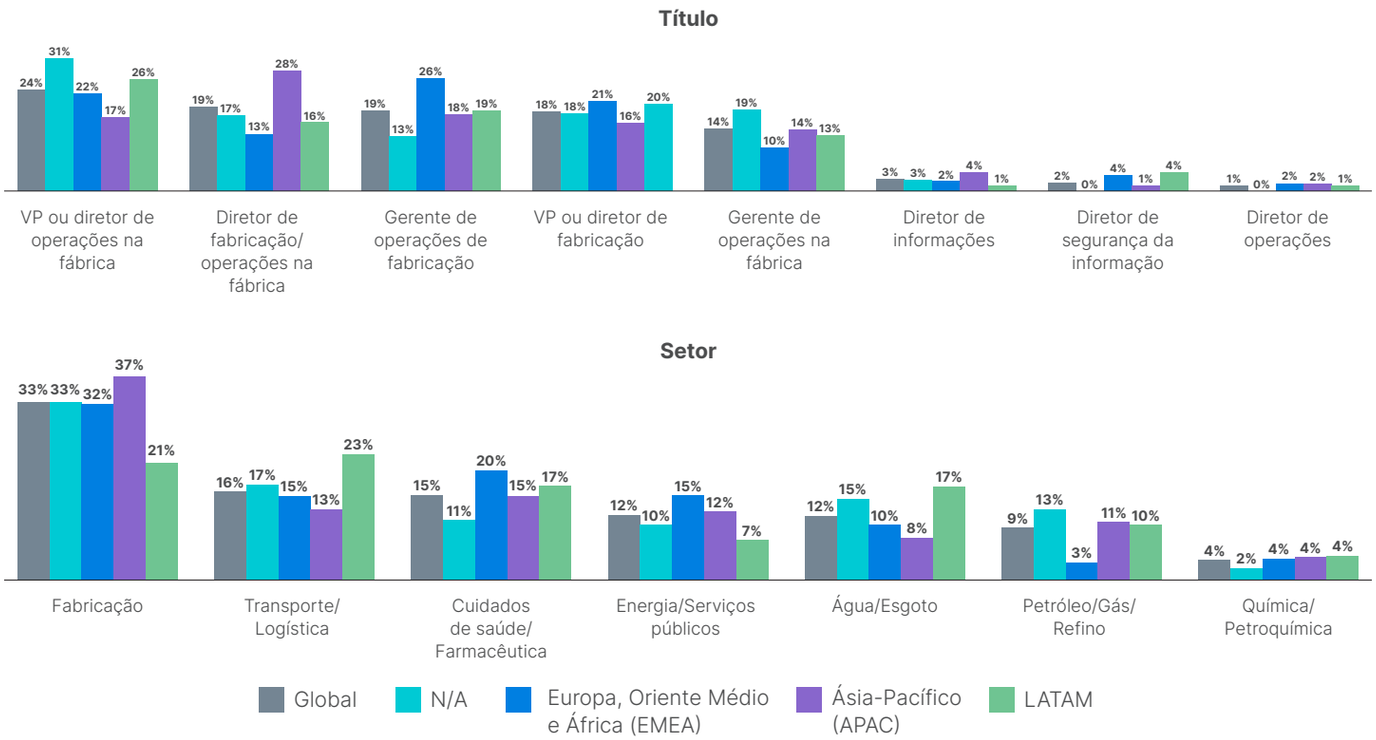



Figura 2: Cargos e setores, por região.

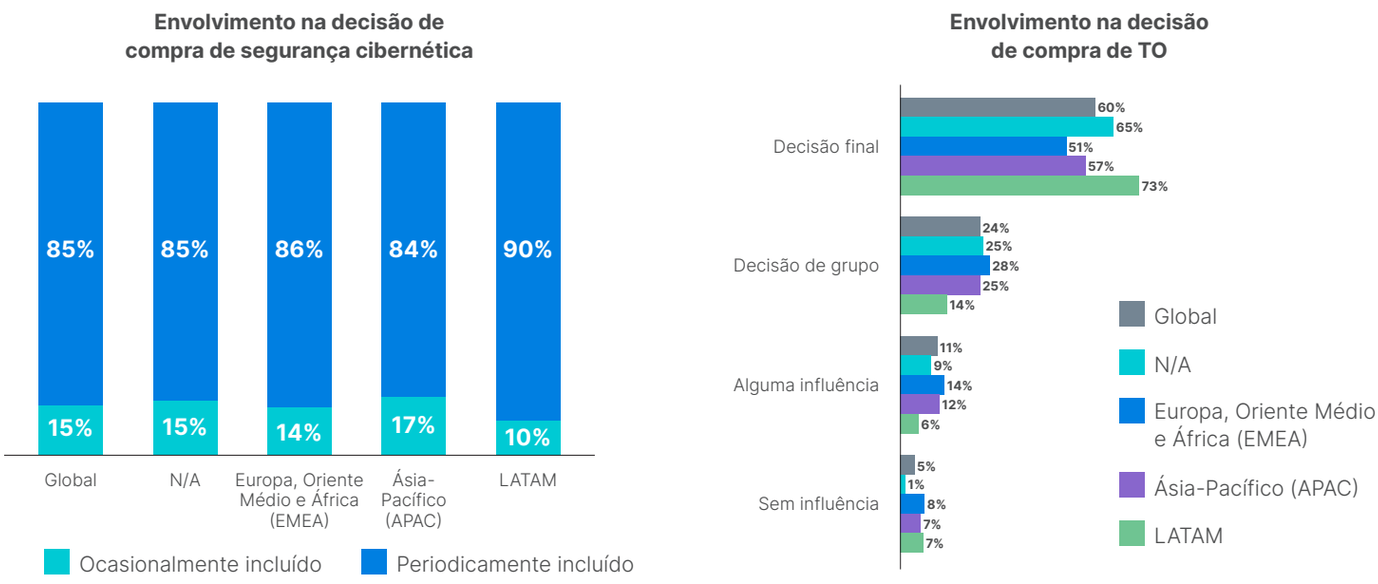



Figura 3: Função dos participantes nas compras de TO e segurança cibernética.

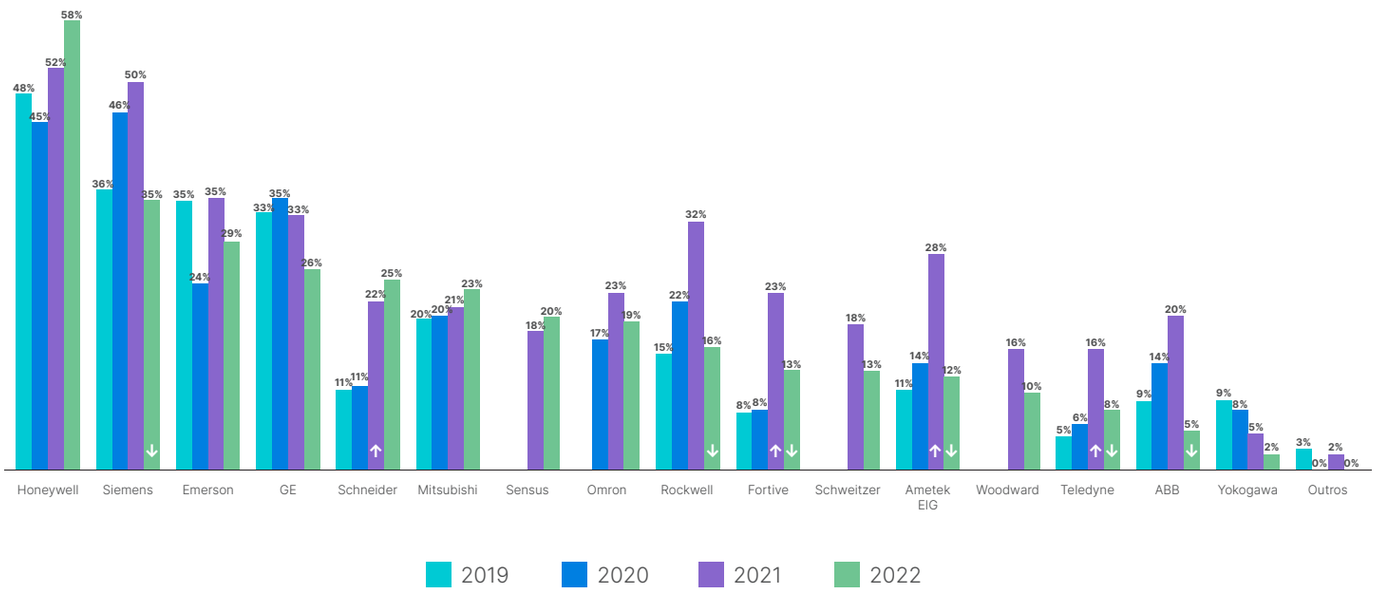



Figura 4: Fornecedores de dispositivos de TO em uso.

### Identificação de conhecimentos e melhores práticas

Este relatório analisa os dados de toda a amostragem e de acordo com a região e o setor. Também comparamos os resultados norte-americanos da pesquisa deste ano com pesquisas semelhantes realizadas na América do Norte em 2019, 2020 e 2021. A partir desta análise, identificamos cinco perspectivas principais sobre o estado atual da segurança cibernética de TO.

Na seção final da pesquisa, analisamos as respostas de acordo com os resultados reais de segurança dos participantes, comparando as organizações que não tiveram invasões durante o ano passado com as que tiveram mais de 10 invasões. Esta comparação resulta em várias melhores práticas às quais as organizações "de alto nível" têm mais probabilidades de aderir.

**"As recentes operações cibernéticas patrocinadas pelo Estado russo incluíram ataques de negação de serviço distribuída (DDoS), e as operações mais antigas incluíram a distribuição de malware destrutivo contra o governo ucraniano e organizações de infraestruturas críticas."[8]**

# Informações para segurança de redes industriais

Os resultados da pesquisa revelam que as organizações têm preocupações crescentes com a segurança de suas infraestruturas de TO, mas que sua preparação para tais ameaças ainda é fragmentada e incompleta. Identificamos cinco perspectivas principais na pesquisa deste ano:

### Perspectiva 1: A segurança de redes industriais é uma preocupação corporativa, e diferentes grupos assumem a responsabilidade

Sem surpresa, a segurança dos sistemas de TO tem a atenção de executivos em muitas organizações, sendo o CTO e o CISO/CSO mais frequentemente citados entre os três principais líderes que influenciam as decisões de segurança cibernética. Contudo, as respostas à pesquisa indicam que tais líderes perderam influência significativa durante o último ano (Figura 5). No ano passado, 50% das organizações classificaram o CTO entre os três principais influenciadores da segurança, e 45% fizeram-no para o CISO/CSO. Tais números diminuíram para 35% e 33%, respectivamente, em 2022. A natureza global da pesquisa não foi um fator de mudança, uma vez que os números foram idênticos para os participantes norte-americanos e para a amostragem global.

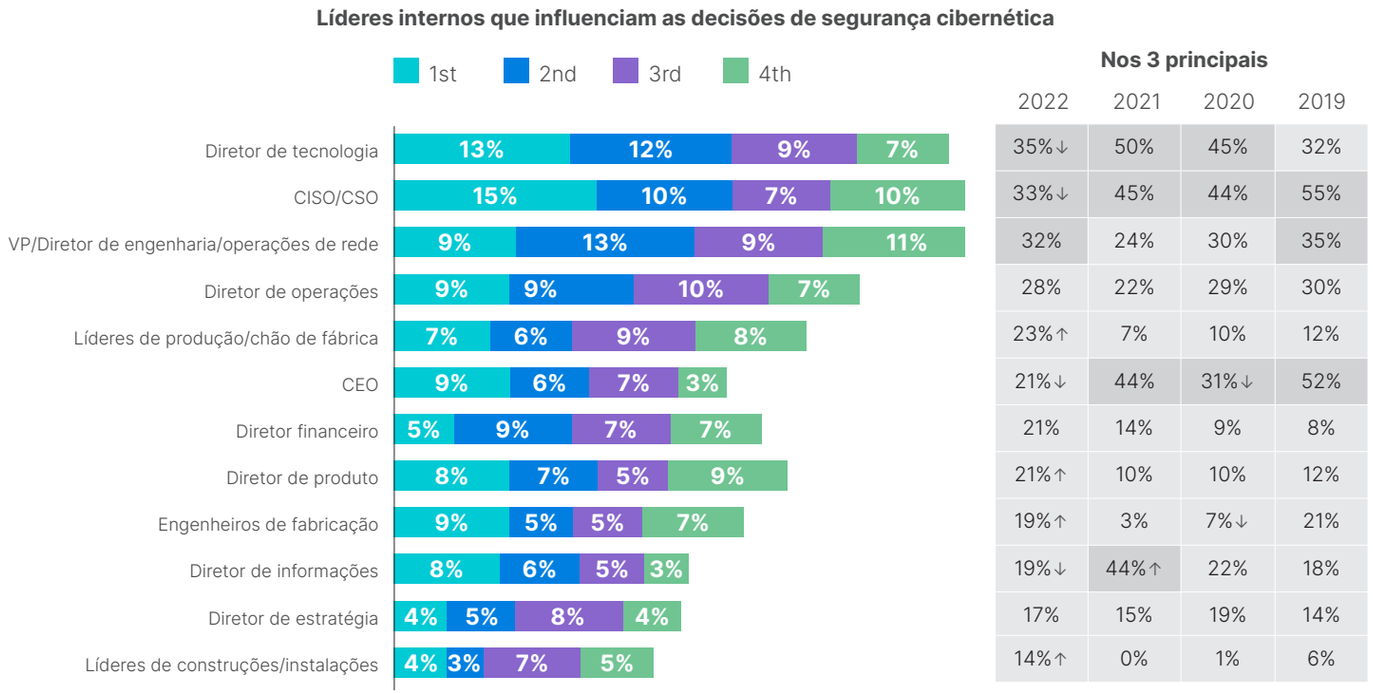



Figura 5: Líderes internos que influenciam as decisões de segurança.

**Quem lidera — e liderará — a segurança de redes industriais?**

Mas quando perguntados sobre quem tem a responsabilidade final pela segurança de redes industriais em suas organizações, um terço dos participantes citou o vice-presidente ou diretor de engenharia ou operações de rede (Figura 6). Este é um grande aumento em relação à porcentagem do ano passado, e o mais elevado nos quatro anos em que a pesquisa é realizada. Indica que a responsabilidade pela segurança de redes industriais pode ter subido um pouco no organograma em comparação aos anos anteriores, quando um diretor ou gerente era responsável pela segurança de redes industriais em diversas organizações.

Há especulações entre os participantes de que este movimento ascendente no organograma continuará. Apenas 15% dos participantes dizem que o CISO detém hoje a responsabilidade pela segurança de redes industriais, mas 79% dizem que esperam que a função se mantenha sob supervisão do CISO durante os próximos 12 meses (Figura 7). No entanto, somos céticos quanto a essa afirmação, uma vez que a grande maioria dos participantes faz esta previsão todos os anos, e a porcentagem de organizações em que o CISO é, atualmente, responsável pela segurança de redes industriais diminuiu ligeiramente em 2022, em comparação com 2021. A influência decrescente do CISO nas decisões de segurança, referida acima, aumenta esse ceticismo.

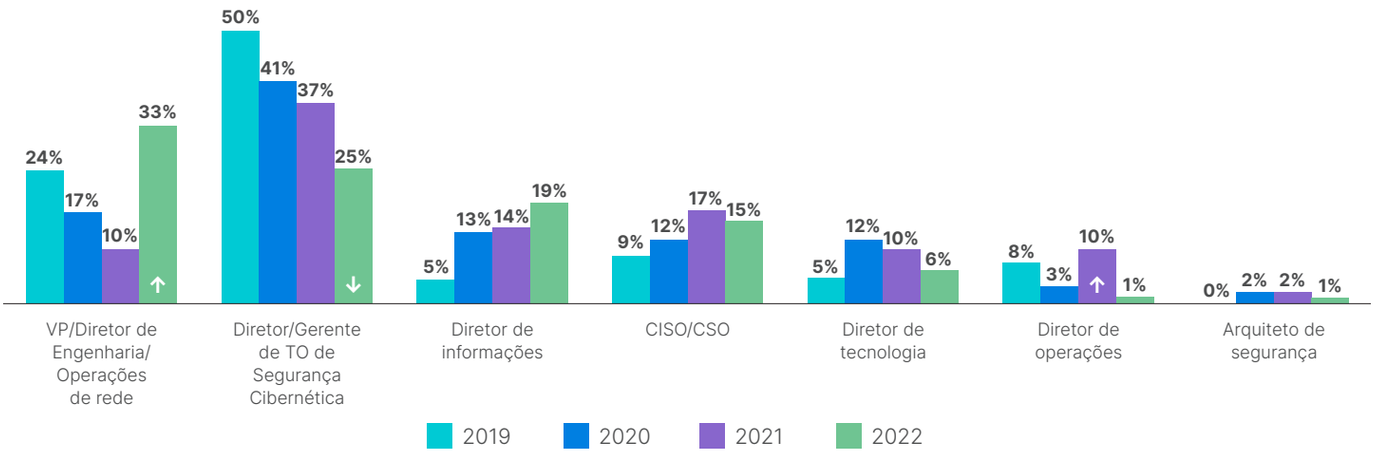



Figura 6: Líder atualmente responsável pela segurança cibernética de TO.

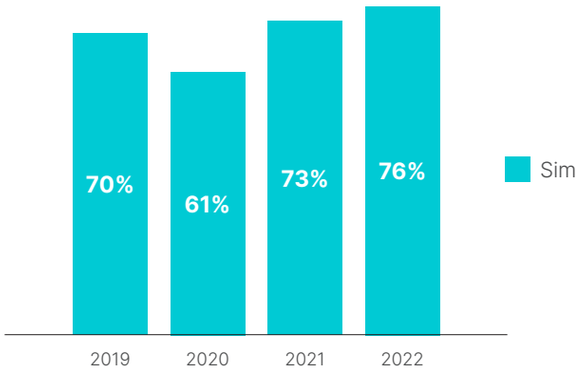



Figura 7: Participantes que esperam que a segurança de redes industriais seja transferida para a supervisão do CISO nos próximos 12 meses.

**Caminhos de carreira para a segurança de redes industriais**

Para se qualificarem a participar da pesquisa, os participantes eram obrigados a ter uma responsabilidade significativa pela TO. De fato, 85% deles passam mais da metade de seu tempo gerindo essa função, e ela consome mais de três quartos das horas de trabalho para 28% (Figura 8). Dois terços dos participantes mundialmente têm um histórico de carreira à parte da TO — quer em organizações industriais ou em fornecedores de soluções de TO (Figura 9). O terço restante provém de um passado de segurança de TI — incluindo mais de metade dos participantes da América Latina.

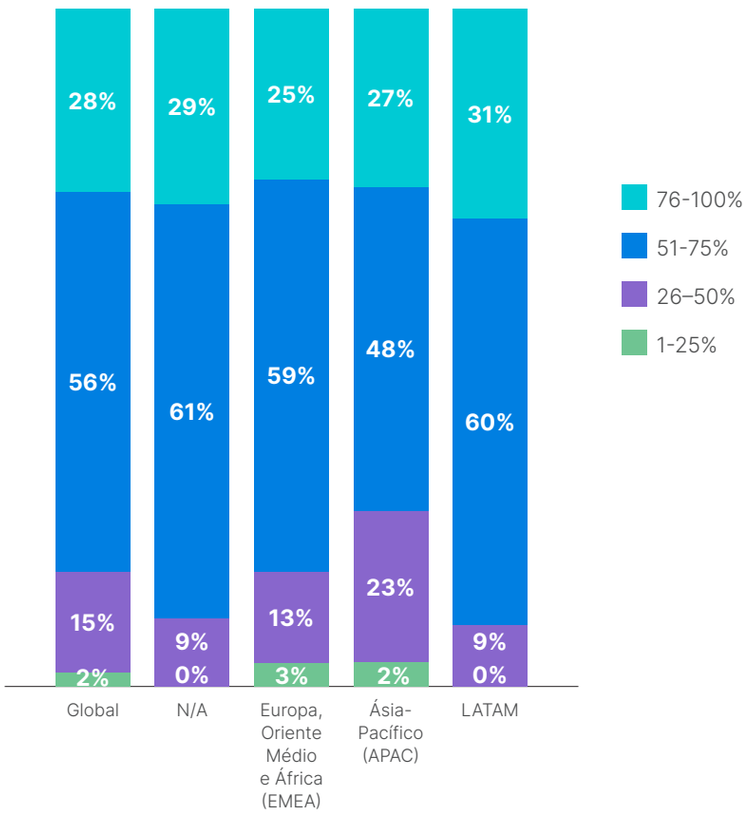



Figura 8: Porcentagem do tempo gasto apoiando/gerindo a segurança de redes industriais.

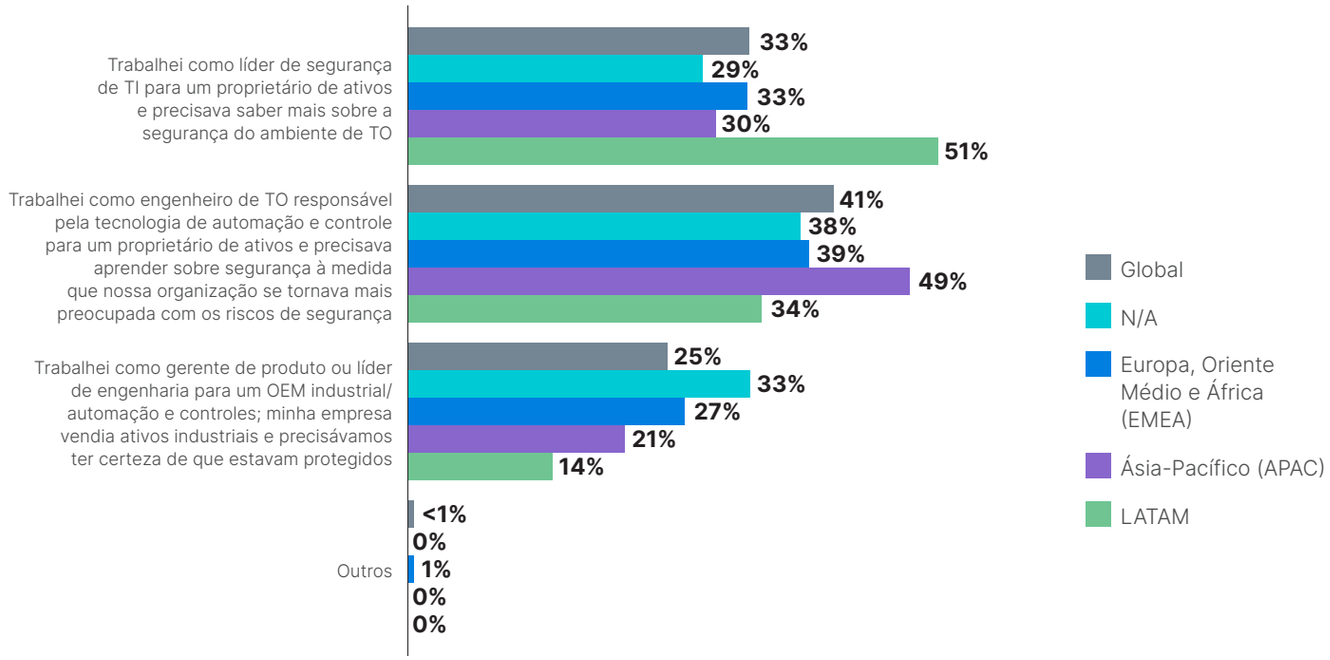
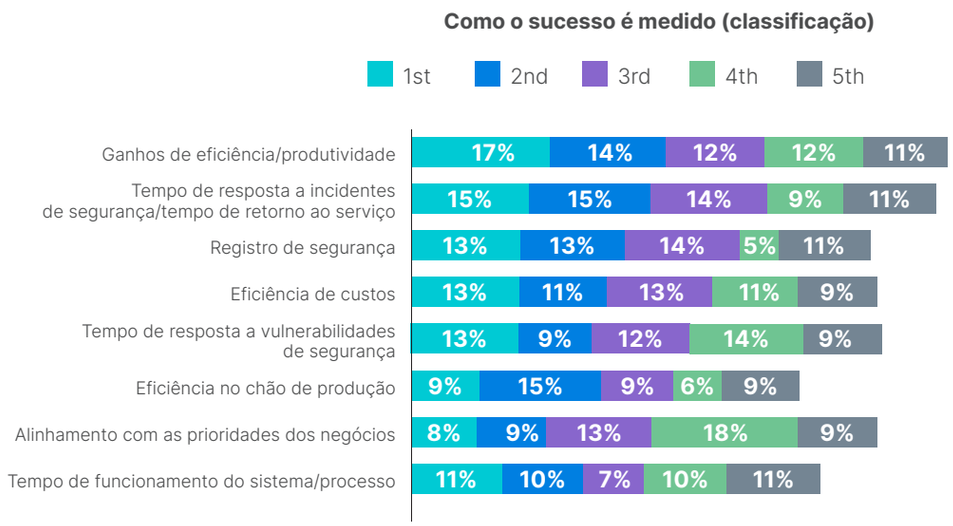



Figura 9: Background na carreira que levou à segurança de redes industriais.

## Perspectiva 2: Algumas organizações ainda tendem a dar prioridade à eficiência em detrimento da segurança de redes industriais

Embora todas as organizações possam afirmar estar preocupadas com a segurança de redes industriais, uma forma de discernir a importância da segurança é analisar como os líderes de TO são avaliados. Na pesquisa deste ano, os ganhos de eficiência e produtividade são ainda mais frequentemente citados como a métrica número um do sucesso, e está entre as três principais em 43% das organizações (Figura 10). Esta avaliação tem sido mais citada como uma das três principais métrica de sucesso todos os anos, mas sua prevalência diminuiu 14% de 2021 para 2022.

**O CISO é um dos principais influenciadores das decisões de segurança dse redes industriais em apenas 33% das organizações, abaixo dos 45% de 2021.**




| | Nos 3 principais | | | |
|---|---|---|---|---|
| | 2022 | 2021 | 2020 | 2019 |
| Ganhos de eficiência/produtividade | 43↓ | 57% | 46% | 55% |
| Tempo de resposta a incidentes de segurança/tempo de retorno ao serviço | 43% | N/A | N/A | N/A |
| Registro de segurança | 40% | 34% | 44% | 41% |
| Eficiência de custos | 37% | 41% | 40% | 53% |
| Tempo de resposta a vulnerabilidades de segurança | 34%↓ | 47%↑ | 32% | 44% |
| Eficiência no chão de produção | 32% | 42% | 41%↓ | 42% |
| Alinhamento com as prioridades dos negócios | 29% | 33% | 24% | 29% |
| Tempo de funcionamento do sistema/processo | 29%↓ | 41% | 40% | 35% |

Figura 10: Ranking de métricas de sucesso.

Ao mesmo tempo, uma métrica de segurança — tempo de resposta a incidentes ou de retorno ao serviço — também foi citada por 43% dos participantes como uma das três primeiras, certamente um bom sinal. Houve também declínios significativos na proeminência do tempo de resposta a vulnerabilidades de segurança e do tempo de funcionamento do sistema/processo, mas o fato de a métrica de resposta a incidentes ser nova para a pesquisa de 2022 pode ser uma das razões de as demais escolhas relacionadas à segurança apresentarem baixa.

### Preocupação específica com ransomware

O ransomware tem dominado as manchetes no espaço da segurança cibernética há vários anos, e as organizações relatam uma preocupação significativa com esta táctica — apesar de ser menos comum do que alguns outros tipos de ataque. Mais de dois terços dos participantes globalmente — e três quartos na América do Norte — afirmam estar mais preocupados com o ransomware do que com outros tipos de invasões (Figura 11). O ransomware tem causado danos significativos e um grande custo econômico ao longo dos anos, e um bom indicador de sua elevada visibilidade é que as organizações estão realmente preocupadas. Contudo, outros tipos de ataques prejudiciais podem não receber a atenção que merecem, por sua menor visibilidade.

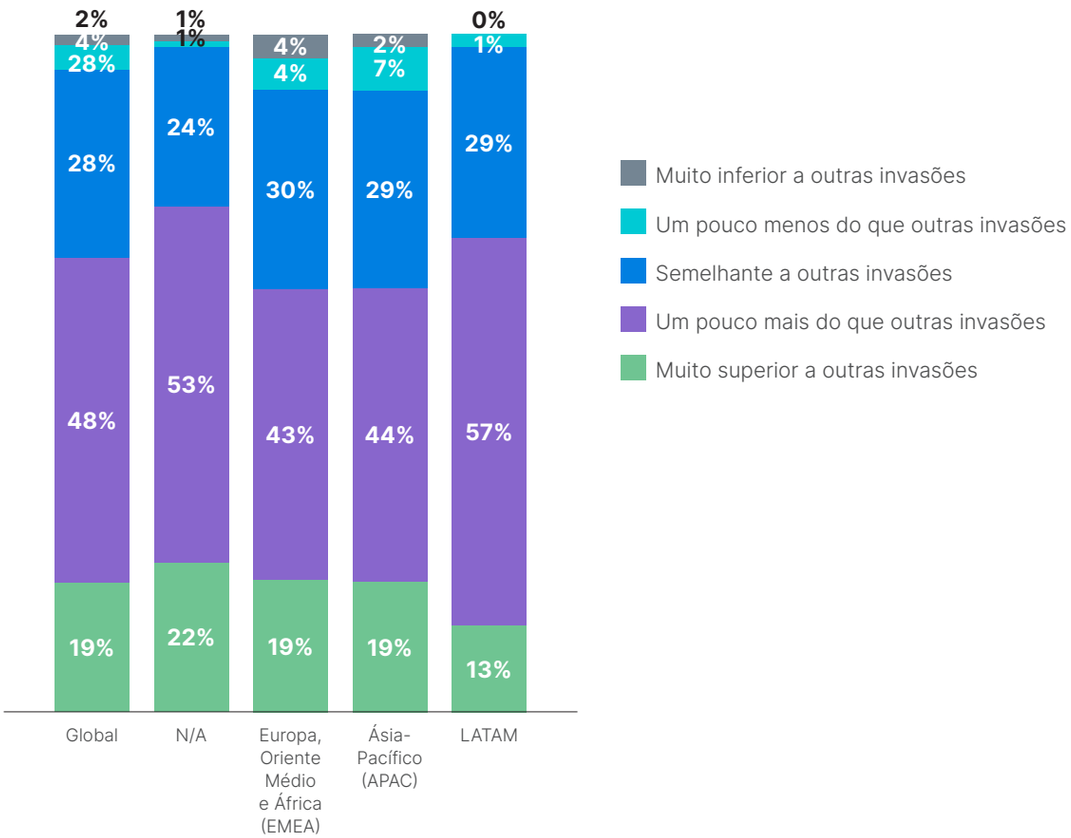



Figura 11: Nível de preocupação com ransomware.

### Classificação da importância das ferramentas de segurança cibernética

Os participantes se encontram em todo o mapa global quanto às soluções de segurança cibernética mais importantes para suas organizações. Análise de segurança, monitoramento e instrumentos de avaliação foram citados como os mais importantes — mas apenas por 17% (Figura 12). Em geral, as soluções de gerenciamento e monitoramento da conformidade foram as mais frequentemente citadas nos três primeiros lugares, e os recursos de proteção de protocolos específicos de TO ficaram em segundo lugar.

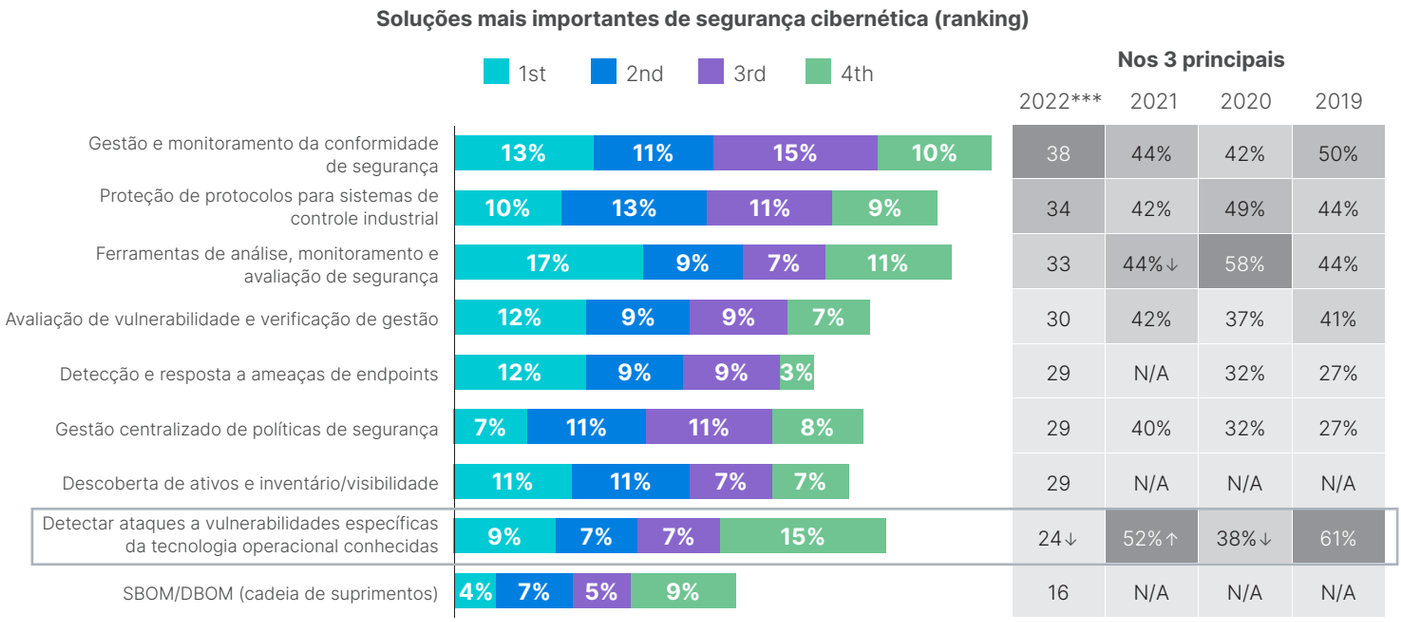



Figura 12: Classificação das mais importantes soluções de segurança cibernética.

## Perspectiva 3: As organizações relatam uma melhoria gradual da postura de segurança de redes industriais, mas são necessárias mais melhorias

Como em anos anteriores, nossa pesquisa pediu que os participantes informassem o nível de maturidade da segurança de redes industriais que suas organizações alcançaram, com uma breve descrição para cada um dos cinco níveis de maturidade. Entre todos os participantes, 84% atingiram pelo menos o nível 2, tendo estabelecido o acesso e a criação de perfis (Figura 13). Metade dos participantes atingiram pelo menos o nível 3, tendo estabelecido um comportamento preditivo, e 21% atingiram o nível 4, com orquestração e automação.

Isto representa uma melhoria marginal com relação a 2021, principalmente por meio de organizações que passaram do nível 2 para o nível 3. A porcentagem de organizações que atingiram pelo menos o nível 3 aumentou de 44% para 50% de um ano ao outro.

**O tempo de resposta a incidentes de segurança/ retorno ao serviço é uma das três principais métricas de sucesso de TO em 43% das organizações.**

Analisando os resultados por região, uma maior proporção de participantes da América Latina e da APAC atingiu o nível 4. Entretanto, na América do Norte, mais organizações saíram do nível 1, mas menos alcançaram o nível 4, deixando mais de 70% das organizações nos níveis médios.

Infelizmente, apenas metade dos participantes dizem que a postura de segurança de redes industriais de sua organização é um fator significativo em sua pontuação global de risco (Figura 14) — embora quase todas as outras organizações a incluam como um fator moderado.

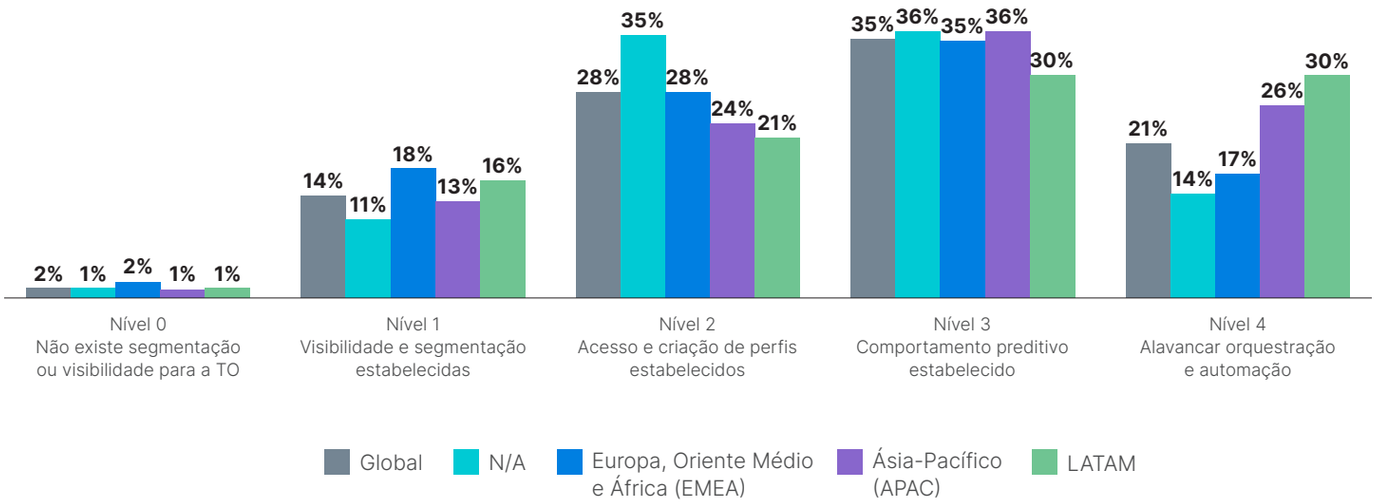



Figura 13: Nível de maturidade da postura de segurança cibernética de TO.

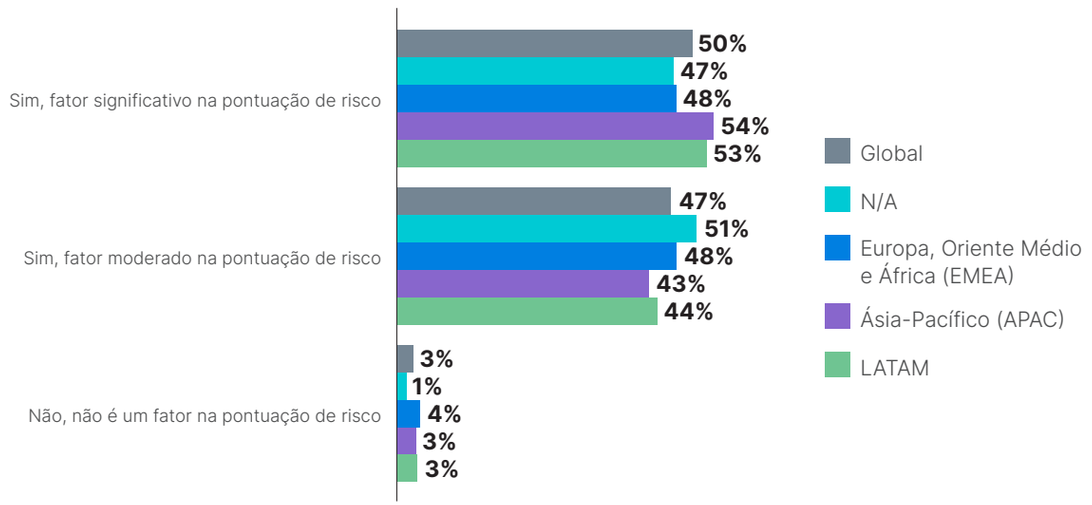



Figura 14: Importância da postura de segurança de redes industriais na pontuação global de risco.

### Maturidade global da segurança cibernética

Os participantes foram também convidados a avaliar a maturidade de seu programa global de segurança cibernética, incluindo TI e TO. Aqui, os participantes tinham maior probabilidade de ter atingido o nível 3 (59%), mas menor probabilidade de ter atingido o nível 4 (16%, Figura 15). Mais uma vez, as empresas latino-americanas e da APAC apresentaram uma maturidade mais elevada enquanto as norte-americanas se mostram globalmente abaixo. As organizações maiores e as do setor de fabricação têm mais probabilidades de ter níveis de maturidade mais elevados, tal como as organizações em que os líderes tecnológicos e de segurança têm influência sobre as decisões de segurança cibernética (Figura 16).

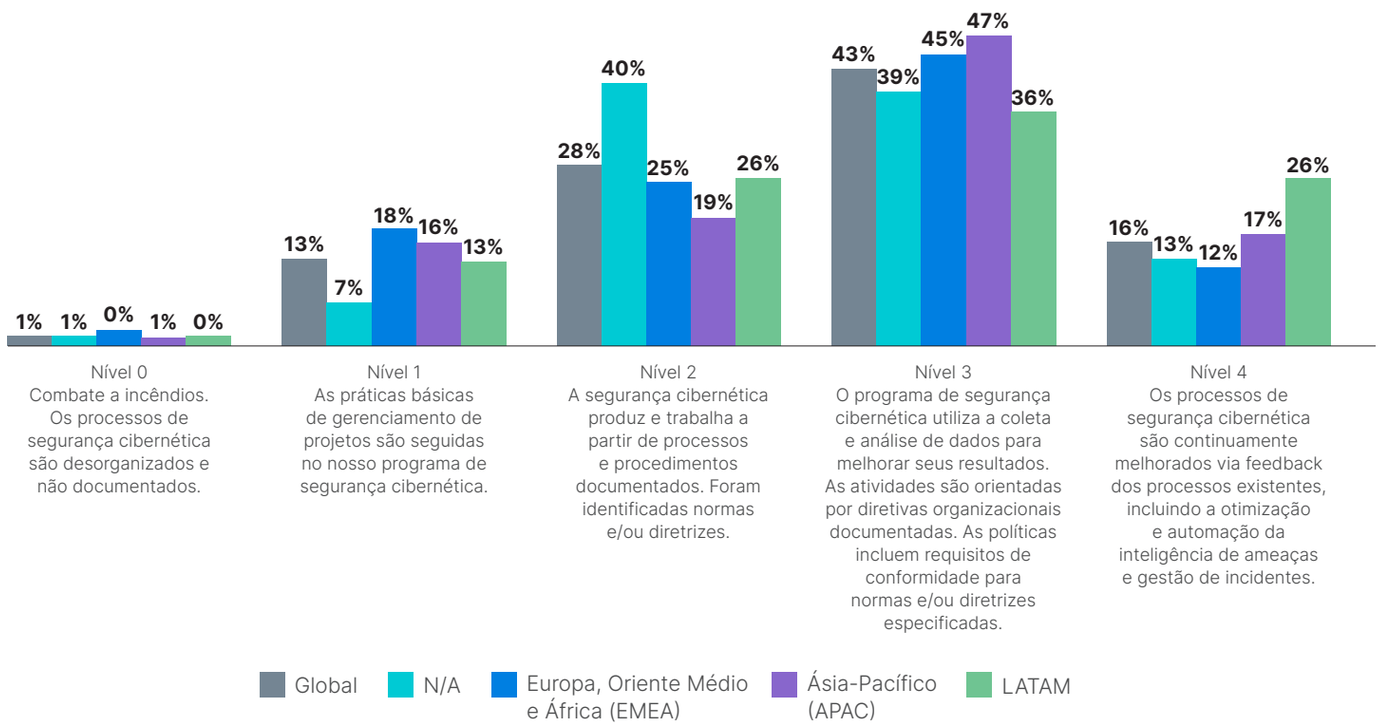
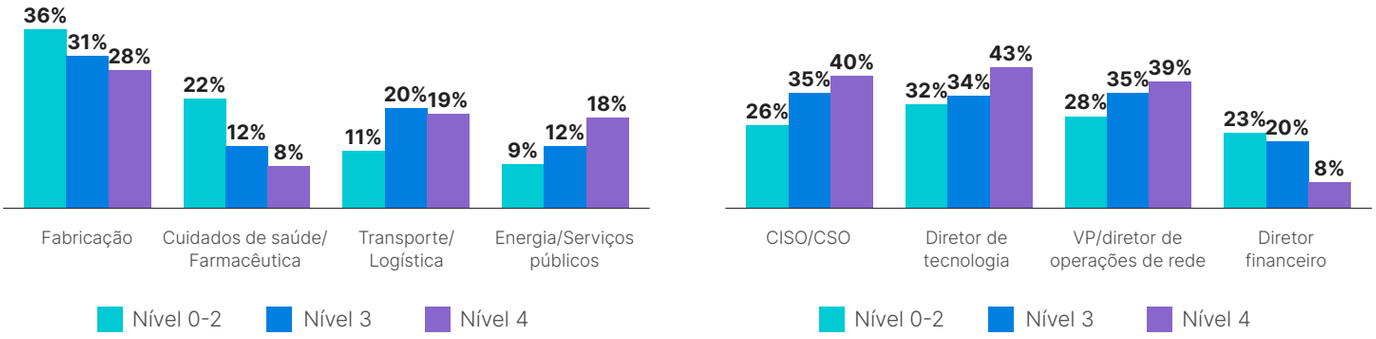



Figura 15: Nível de maturidade do programa global de segurança cibernética.




| % mais de 5.000 funcionários | | |
|---|---|---|
| 21% | 28% | 41% |

| % de apoio/impedimento de segurança cibernética em meu sucesso | | |
|---|---|---|
| 65%/4% | 82%/6% | 83%/11% |
| **% de apoio ao facilitar padrões de segurança** | | |
| 40% | 46% | 58% |

Figura 16: Demografia selecionada dos participantes por nível de maturidade do programa de segurança cibernética.

### Visibilidade centralizada

O estabelecimento da visibilidade dos processos de TO está incluído no nível 1 da nossa matriz de maturidade de segurança de redes industriais, mas a granularidade dessa visibilidade pode fazer a diferença. Enquanto 98% dos participantes reivindicam pelo menos o nível 1 de maturidade de segurança de redes industriais, apenas 74% dizem que mais de três quartos de suas atividades de TO estão visíveis para a equipe de operações de segurança (Figura 17). Este número é de 77% na América do Norte, uma melhoria em relação aos resultados de pesquisas norte-americanas dos últimos anos (Figura 18). No entanto, a porcentagem de participantes norte-americanos com 100% de visibilidade parece estar em declínio — de 23% em 2020 para 13% em 2022.

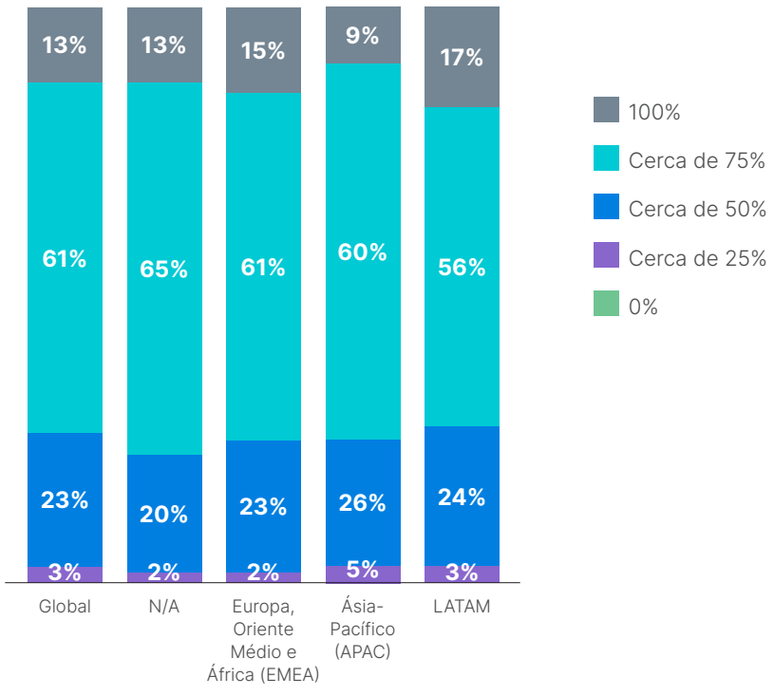



Figura 17: Visibilidade das atividades de TO por operações de segurança.

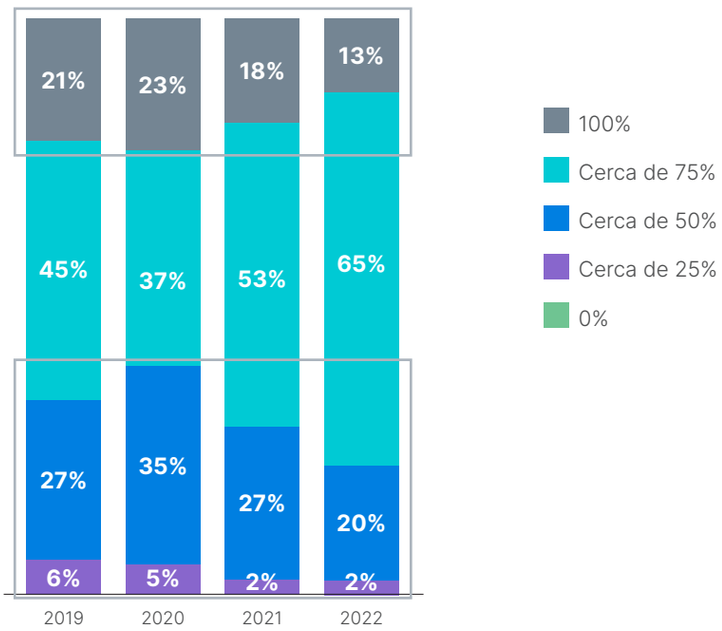



Figura 18: Visibilidade das atividades de TO por operações de segurança, América do Norte.

## Perspectiva 4: As organizações têm diversas formas de abordar a segurança de redes industriais, e muitas têm lacunas de segurança

Como os sistemas de TO estiveram muitas vezes isolados da internet nos últimos anos, a necessidade de protegê-los das ameaças de TI é relativamente nova, e nossa pesquisa concluiu que as práticas de segurança ainda não foram padronizadas.

Como temos discutido, uma abordagem é confiar o gerenciamento da segurança de redes industriais ao SOC, que tem cumprido essa função para os sistemas de TI há anos. Quase todos os participantes adotaram essa abordagem para pelo menos algumas atividades de TO, mas apenas 52% das organizações conseguiram permitir monitoramento e acompanhamento de *todas as* atividades de TO pela equipe do SOC (Figura 19). Isto se mantém essencialmente inalterado ao longo dos quatro anos em que realizamos a pesquisa. As empresas da APAC estão se saindo um pouco melhor neste quesito, com 59% monitorando todas as atividades via SOC.


**50% das organizações atingiram o nível 3 de maturidade de segurança de redes industriais — acima dos 44% de 2021.**

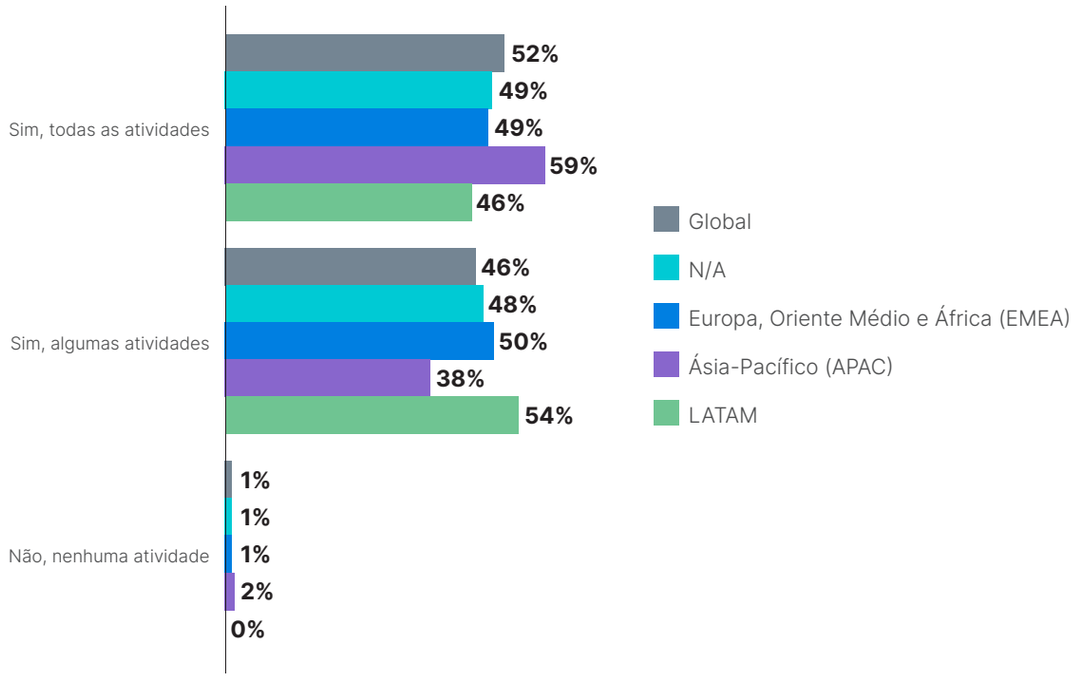



Figura 19: Atividades de TO monitoradas e acompanhadas pelo SOC.

### Métricas rastreadas e comunicadas

Quando se trata de rastrear e informar métricas de segurança, os resultados são mistos. Quando apresentados a uma lista de medidas básicas de segurança cibernética que, provavelmente, deveriam ser seguidas em cada organização, não mais de 52% dos participantes afirmaram estar seguindo alguma delas (Figura 20).

Comparando os resultados norte-americanos com os anos anteriores, a porcentagem que acompanha e informa várias das métricas diminuiu significativamente a partir de 2021 (Figura 21) — incluindo vulnerabilidades encontradas e bloqueadas e invasões detectadas e sanadas.

Porcentagens semelhantes de participantes informam informações básicas de segurança de redes industriais periodicamente à gerência executiva. Apresentados a uma lista que inclui informações críticas como relatórios de conformidade, avaliações de segurança e comprometimentos de segurança, não mais de 53% informaram qualquer item à gerência executiva (Figura 22).

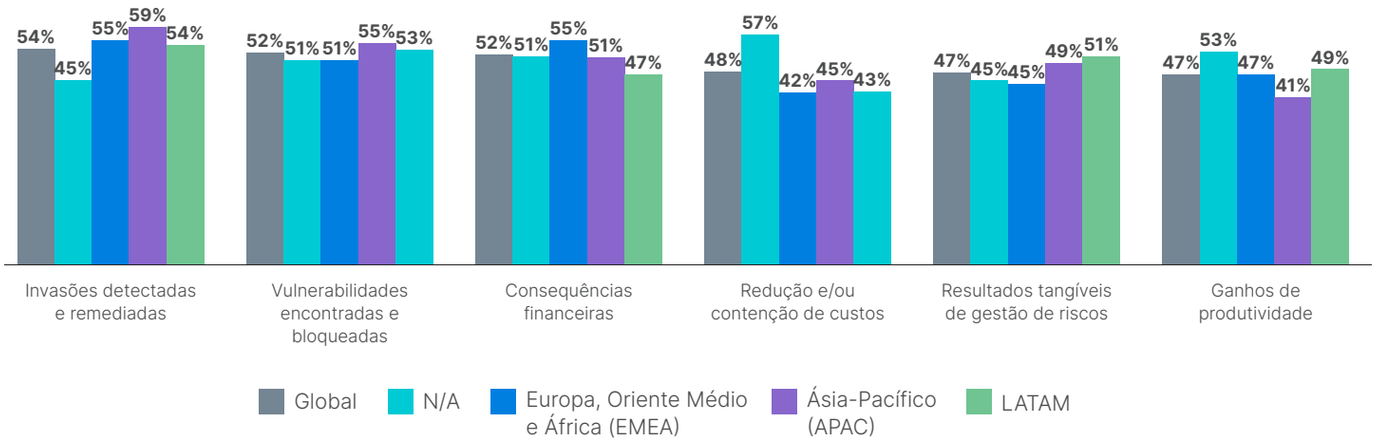



Figura 20: Métricas de segurança cibernética monitoradas e mencionadas.

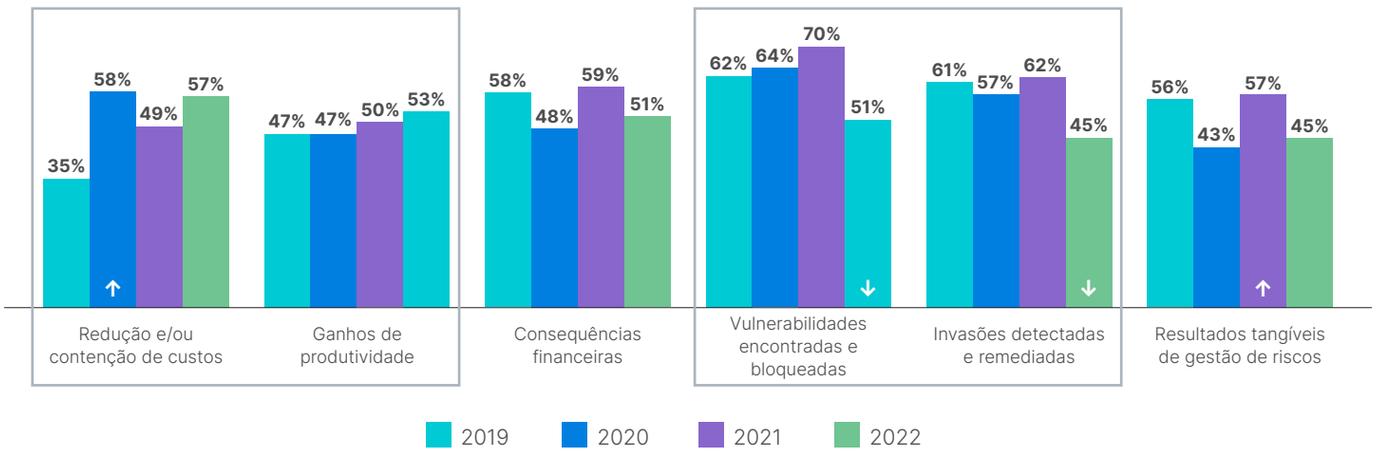



Figura 21: Medidas de segurança cibernética acompanhadas e relatadas, América do Norte.

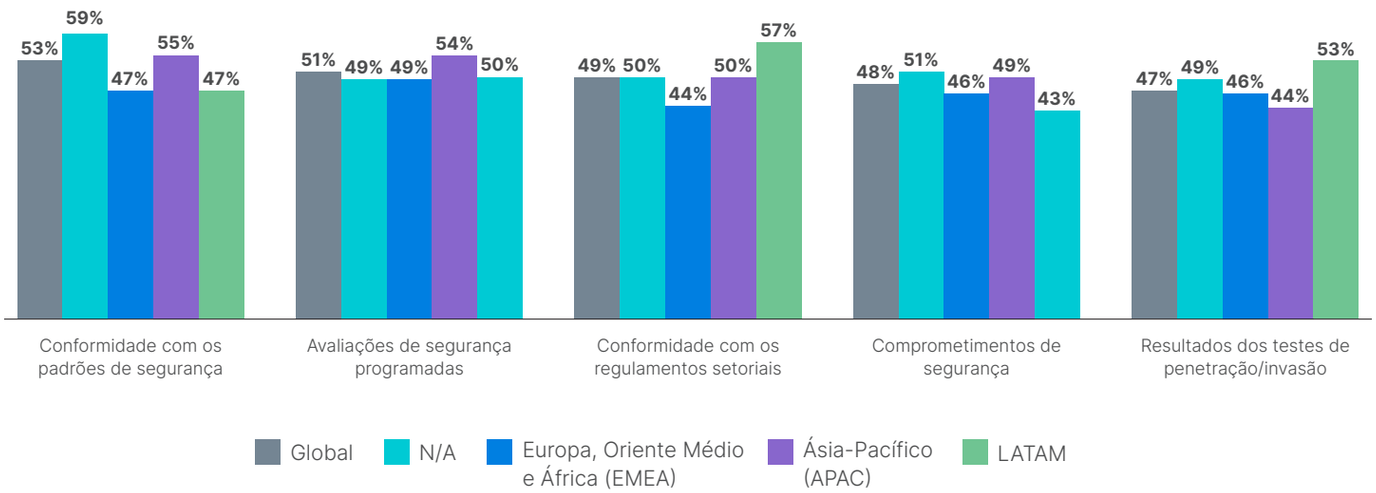



Figura 22: Questões de segurança cibernética de TO comunicadas à gerência executiva.

## Recursos de segurança em uso

Os participantes deram diversas respostas relativamente às ferramentas e recursos de segurança que utilizam para proteger seus sistemas de TO. Apresentados a uma lista bastante abrangente de ferramentas e processos, nenhum recurso é utilizado por mais de 47% dos participantes (Figura 23). As soluções incluídas pela primeira vez este ano incluem acesso remoto seguro (41%); orquestração, automação e resposta de segurança (SOAR; 37%); e a utilização de inteligência de ameaças (36%).

Esta abordagem de "algumas das anteriores" reflete um aspecto da segurança que, em muitos sentidos, está ainda em sua infância, com diferentes organizações tentando abordagens diferentes. Uma prática que está claramente diminuindo sua popularidade é a utilização do centro de operações de rede (NOC) para o gerenciamento da segurança de redes industriais (Figura 24). Curiosamente, os participantes norte-americanos tenderam, de forma geral, a utilizar menos os recursos e práticas listados.

**Não mais de 47% das organizações utilizam qualquer ferramenta ou abordagem de segurança de redes industriais.**

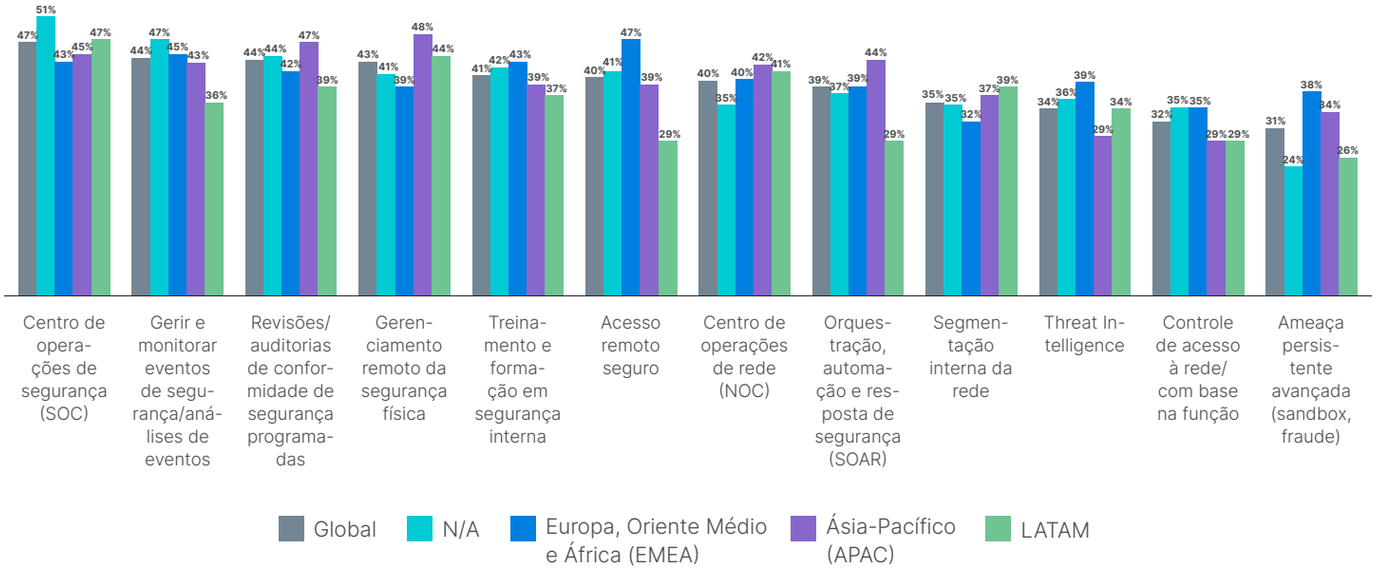



Figura 23: Segurança cibernética e recursos de segurança em vigor.

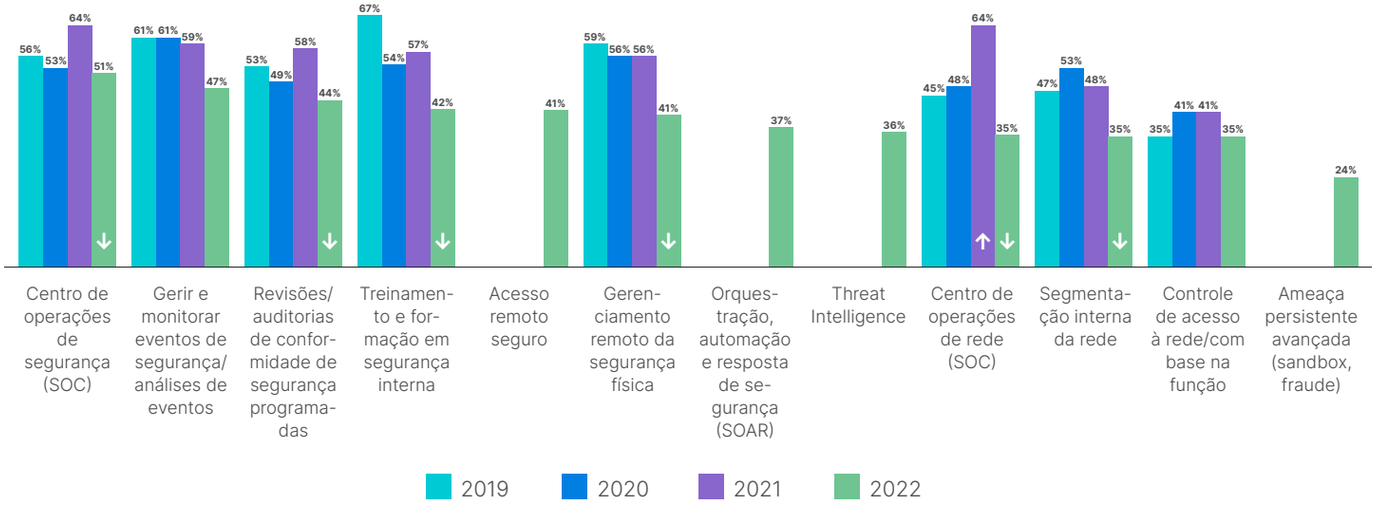



Figura 24: Segurança cibernética e recursos de segurança em vigor, América do Norte.

### Complexidade dos sistemas de segurança e percepção da eficácia

A complexidade é uma questão que pode impedir a segurança de redes industriais. A grande maioria das organizações utiliza entre dois e oito fornecedores diferentes para seus dispositivos de TO, e tem entre 100 e 10.000 dispositivos em funcionamento (Figura 25). Apenas 7% das organizações tiveram sucesso na redução para um do número de fornecedores.

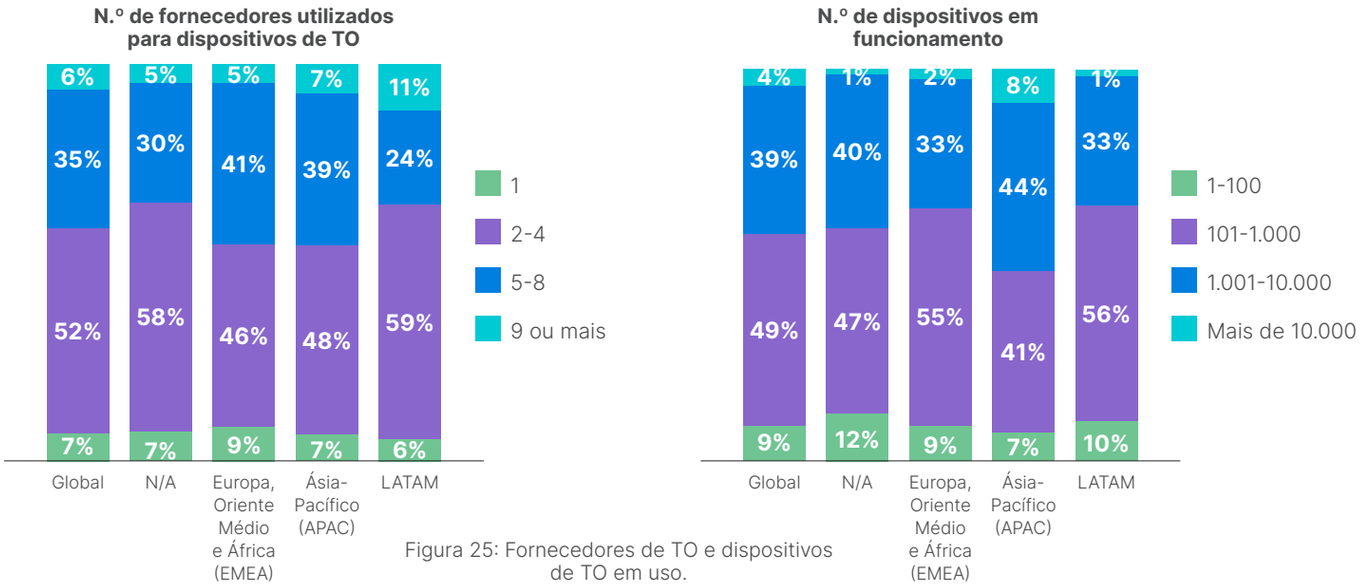



Figura 25: Fornecedores de TO e dispositivos de TO em uso.

## Perspectiva 5: A maioria das organizações ainda sofre várias invasões anualmente

Todos os anos, fazemos aos participantes uma simples pergunta sobre seus resultados em termos de segurança: quantas invasões ocorreram ao longo dos últimos 12 meses. Em 2022, três quartos dos participantes admitiram pelo menos três invasões, 19% tiveram mais de seis, e 7%, mais de 10 (Figura 26). Apenas 6% dos participantes declararam não ter sofrido invasões nos últimos 12 meses.

Olhando para os resultados norte-americanos desta questão ao longo de quatro anos, as coisas não estão melhorando no geral, com aproximadamente a mesma porcentagem de três ou mais invasões desde 2020 (Figura 27). Um pequeno consolo é que a porcentagem de participantes norte-americanos que tiveram 10 ou mais invasões diminuiu de 12% para 5% de um ano para o outro.

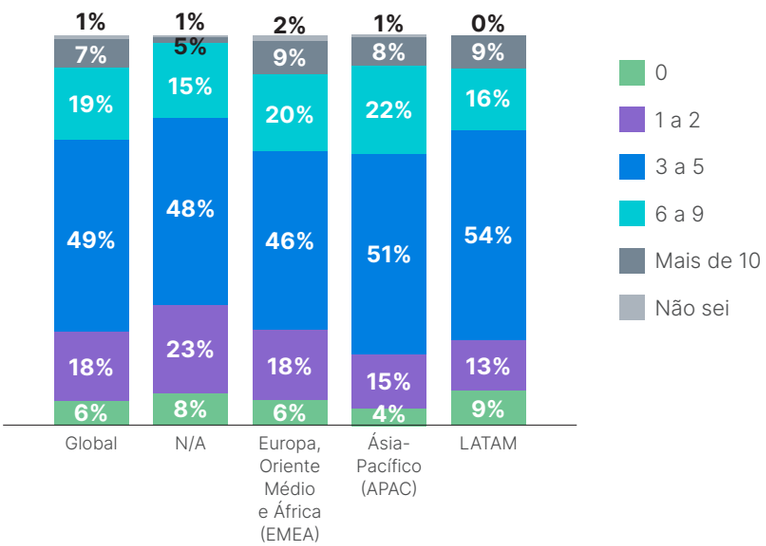



Figura 26: Número de invasões no ano passado.

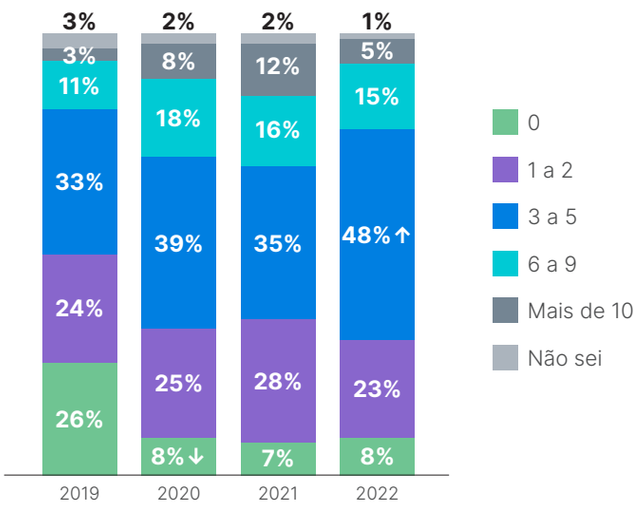



Figura 27: Número de invasões no último ano, América do Norte.

### Tipos de ataques

Os participantes sofreram uma grande variedade de tipos de ataques — o que não é surpreendente dado o número de invasões. Um total de oito tipos de ataque afetou pelo menos um quarto dos participantes, com malware e phishing no topo da lista, atingindo mais de 40% das organizações (Figura 28). O ransomware atingiu menos de um terço das organizações em geral, mas 44% das empresas latino-americanas. E menos participantes latino-americanos sofreram phishing do que nas outras regiões. Olhando para os resultados norte-americanos ao longo de quatro anos, malware e violações maliciosas de informação privilegiada mostraram declínios este ano (Figura 29).

Apesar de o número global de invasões ser notavelmente semelhante, não obstante o nível de maturidade de segurança relatado — provavelmente porque as organizações mais maduras são capazes de detectar uma maior porcentagem de invasões. Mas olhando para isso por tipo de ataque, fica claro que as organizações mais maduras têm menos problemas com ameaças internas, ao mesmo tempo que detectam mais ataques do exterior (Figura 30).

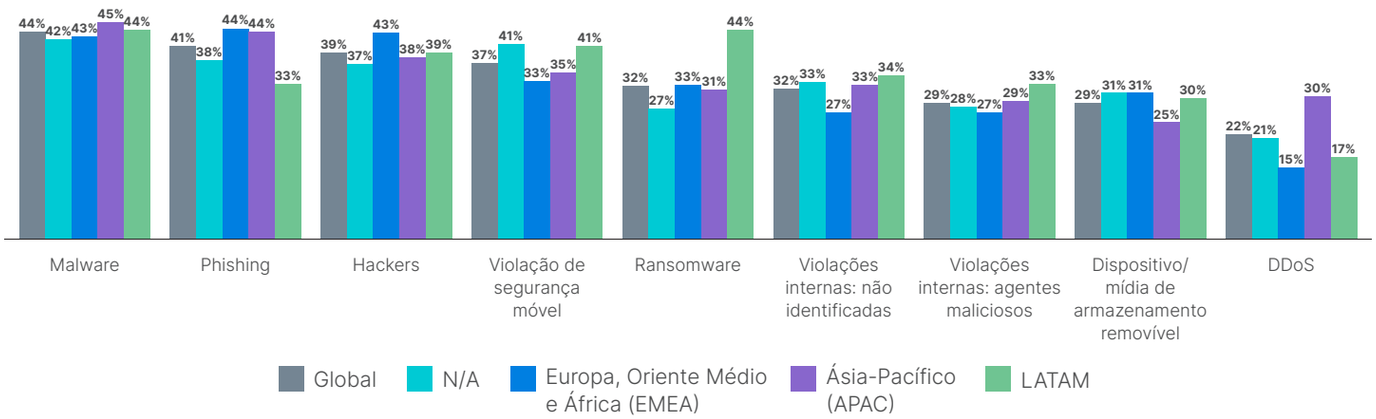



Figura 28: Tipos de invasões sofridas.

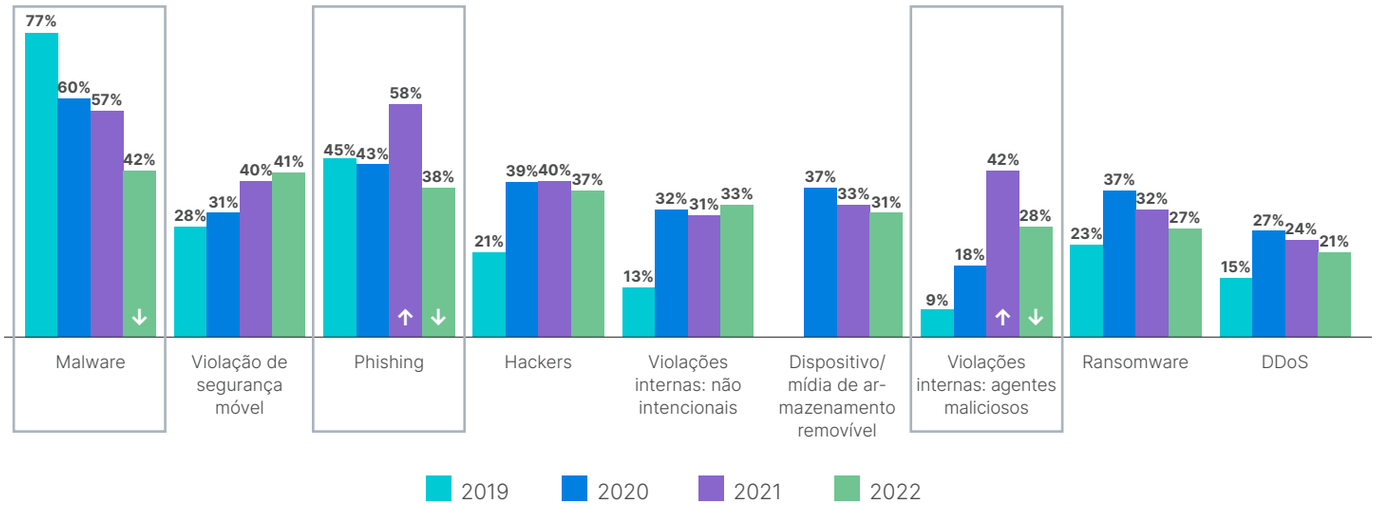



Figura 29: Tipos de invasões sofridas, América do Norte.

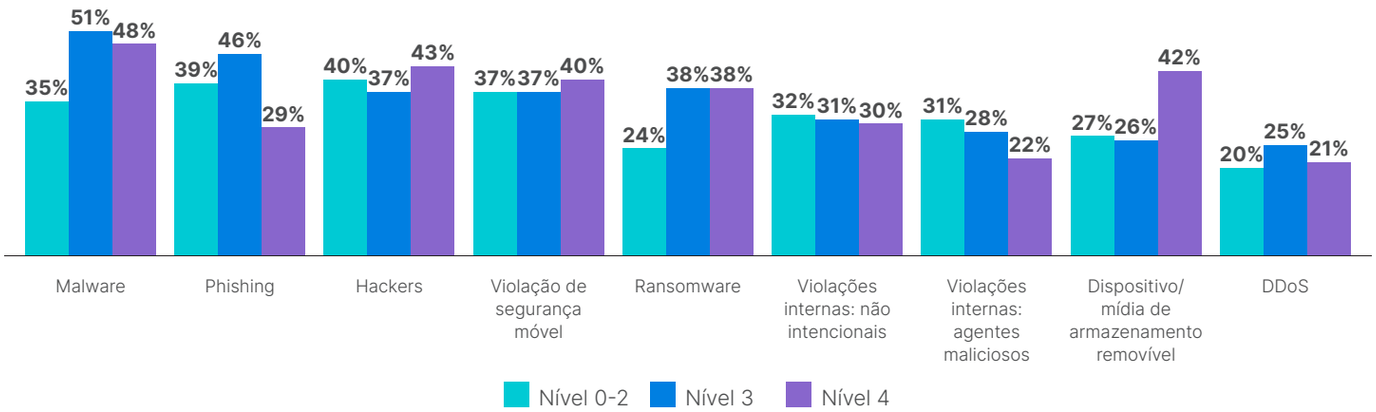



Figura 30: Tipos de invasões sofridas por nível de maturidade de segurança informado.

### Impacto dos ataques

Curiosamente, uma porcentagem ligeiramente mais elevada de ataques afetou sistemas de TO em relação aos sistemas de TI (Figura 31), com 61% das invasões impactando a TO e 60%, a TI. Os impactos comerciais das invasões não foram, de forma alguma, triviais. Cerca de metade dos participantes sofreu uma interrupção operacional que afetou a produtividade, enquanto mais de um terço viu perdas de receitas e dados, problemas de conformidade e impactos sobre o valor da marca — e até mesmo ameaças à segurança física (Figura 32). E 90% dos participantes admitem que o retorno ao serviço foi um processo que levou horas ou ainda mais tempo (Figura 33).

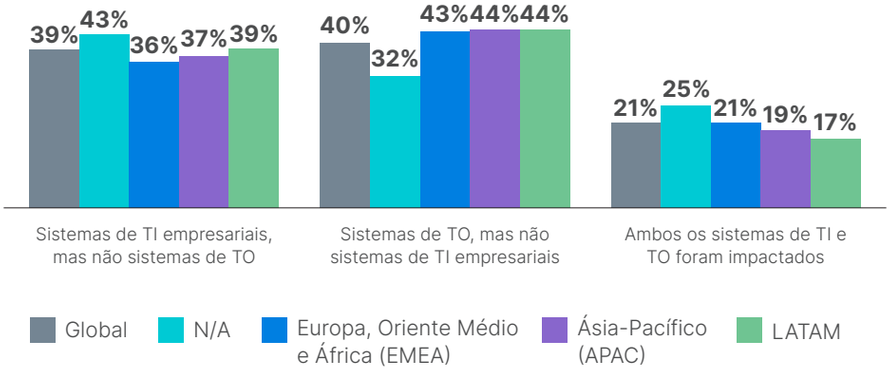



Figura 31: Ambientes impactados por invasões.

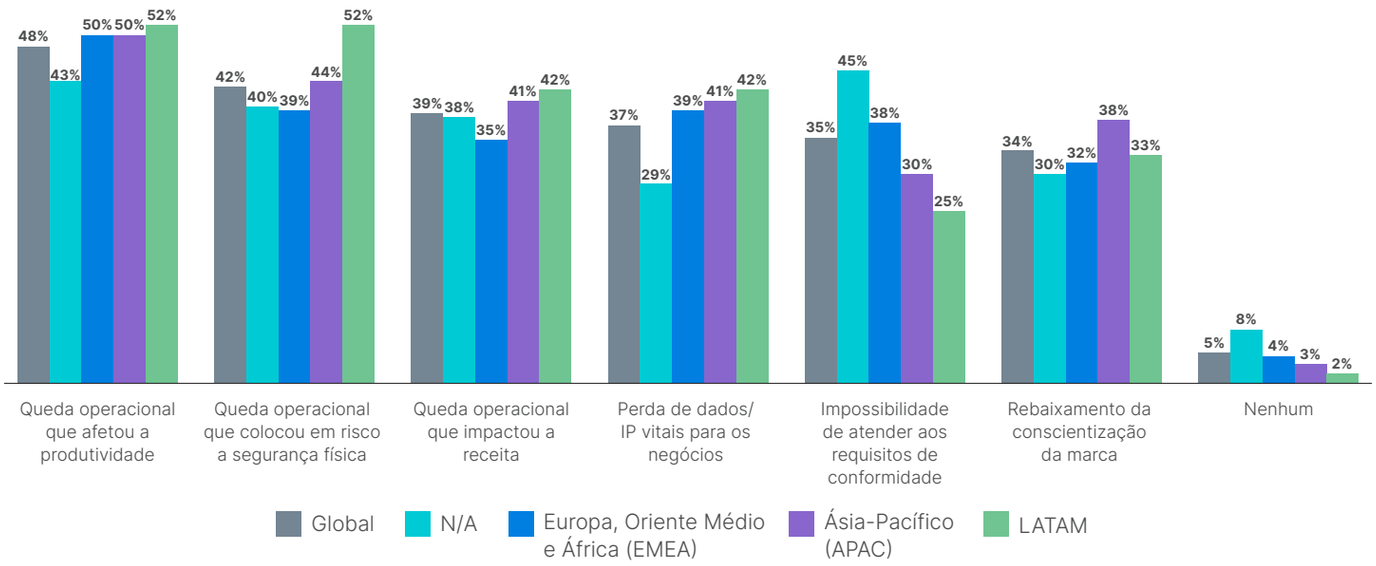



Figura 32: Impactos organizacionais das invasões.

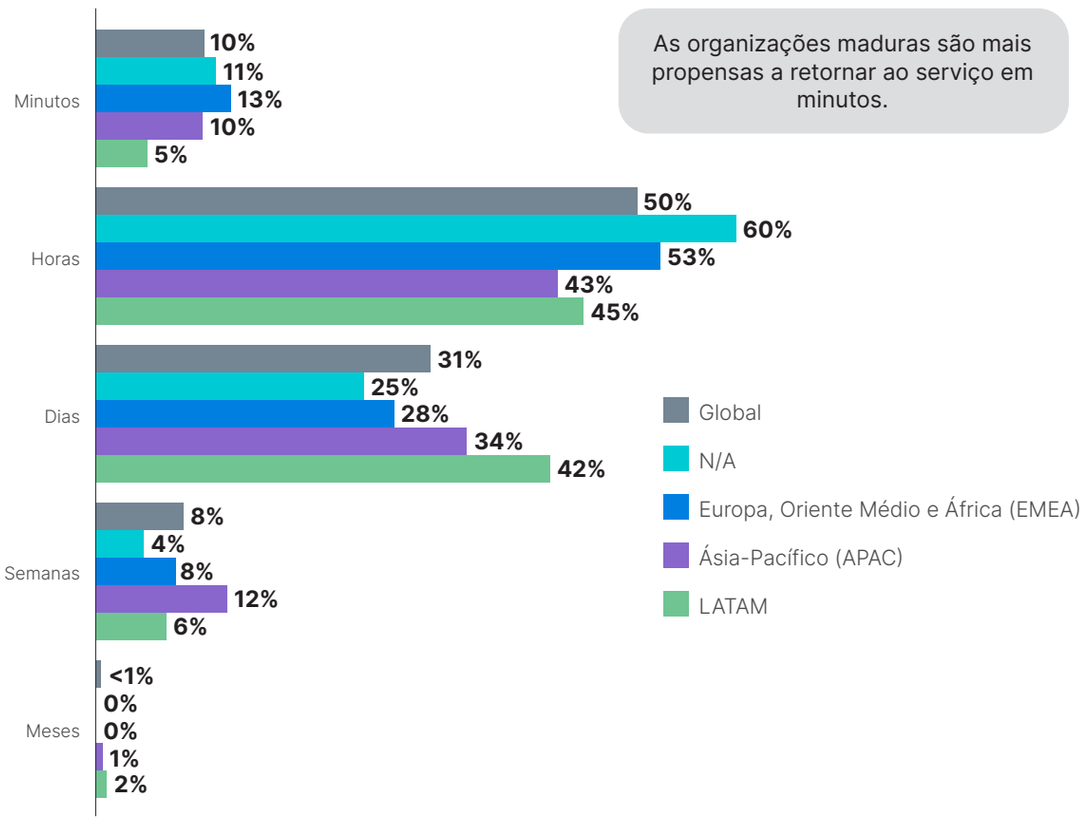



Figura 33: Retorno mais longo ao serviço após uma invasão.

# Melhores práticas para as organizações de alto nível

Apenas 6% das organizações representadas na pesquisa deste ano afirmam não ter tido invasões nos últimos 12 meses, enquanto 5% citaram *mais de 10 invasões.* Comparamos as práticas.


Apenas 6% dos participantes puderam reivindicar zero invasões no ano passado.

## 1. As organizações de alto nível têm 17% mais probabilidades de ter todas as suas atividades de TO centralmente visíveis para as operações de segurança cibernética.

A visibilidade centralizada e de ponta a ponta de todas as atividades de TO é fundamental para garantir sua segurança, e este é definitivamente um trabalho em curso na maioria das organizações. As organizações de alto nível têm mais que o triplo de probabilidade de ter tal visibilidade do que suas congêneres de nível inferior.

## 2. As organizações de alto nível têm 177% mais probabilidades de ter um tempo de resposta de vulnerabilidade de segurança como uma de suas três principais métricas de sucesso.

Como diz o velho ditado, "o que se mede, melhora", e responder rapidamente às vulnerabilidades de segurança de redes industriais é crucial para proteger tais sistemas. As organizações com melhores resultados têm quase três vezes mais probabilidades de ter esta métrica como parte importante de sua revisão de desempenho.

## 3. As organizações de alto nível têm 37% mais probabilidades de disporem de tecnologia de controle de acesso à rede com base na função.

Garantir que apenas as partes autorizadas possam acessar sistemas específicos é fundamental para proteger qualquer ativo tecnológico. Quando se trata de TO, as pessoas que necessitam de acesso a tais sistemas estão em uma gama relativamente limitada de cargos. As organizações que evitaram invasões no ano passado são muito mais propensas a ter tais controles em vigor.

## 4. As organizações de alto nível têm 48% mais probabilidades de denunciar comprometimentos de segurança à liderança sênior/executiva.

Os itens incluídos nos relatórios periódicos à liderança executiva tendem a permanecer na mente durante todo o ano. As organizações que mantêm os líderes de alto nível informados sobre os comprometimentos de segurança tendem a sofrer menos comprometimentos. As organizações de alto nível tendem a ser mais transparentes com a gerência executiva.

## 5. As organizações de alto nível têm 32% mais probabilidades que seu SOC monitore e rastreie a segurança de redes industriais.

Os centros de operações de segurança (SOCs) existem há décadas e desenvolveram melhores práticas granulares para o gerenciamento da segurança de TI. Os líderes de TO que evitaram invasões são mais suscetíveis a confiar a segurança de redes industriais ao mesmo grupo.

## 6. Organizações de alto nível são 44% mais propensas a rastrear e informar invasões detectadas e sanadas.

Compreender os ataques anteriores aumenta as capacidades de uma organização de frustrar ataques futuros, e isso começa com a preservação de registros. As organizações que evitaram invasões são mais suscetíveis de as informar rotineiramente quando elas ocorrem.

## 7. As organizações de alto nível são infinitamente mais propensas a utilizar apenas um fornecedor para seus dispositivos de TO habilitados para IP.

Evitar a complexidade nas redes e sistemas é uma boa forma de reduzir a superfície de ataque e melhorar a postura de segurança. Nenhuma das organizações que sofreram 10 ou mais invasões utilizava apenas um fornecedor para seus dispositivos de TO com IP, enquanto quase um terço das organizações de alto nível tinha obtido isto.

# Conclusão

O Relatório sobre o estado da tecnologia operacional e da segurança cibernética de 2022 constata que os esforços de segurança de redes industriais em organizações em todo o mundo estão fazendo progressos inadequados no sentido da proteção total dos sistemas ICS e SCADA no mundo relativamente novo da TO conectada. O progresso que tem sido feito com relação à maturidade da segurança desde o ano passado pouco melhorou os resultados reais da segurança. A consequência é que a grande maioria das organizações continua sofrendo invasões — múltiplas vezes por ano, na maioria dos casos.

Dado o clima geopolítico, os governos de todo o mundo estão advertindo que é provável que haja um aumento dos ataques cibernéticos a infraestruturas críticas e a ativos econômicos essenciais. As organizações industriais de um largo espectro de setores farão bem em avançar rapidamente a maturidade de seus esforços de segurança de redes industriais, alavancando o comportamento preditivo, a orquestração e tecnologias de automação para estabelecer um verdadeiro acesso de confiança zero e se proteger contra ameaças vindas de infiltrados mal-intencionados e bem-intencionados, criminosos cibernéticos externos e ataques patrocinados por um governo.

# Lista de referência

[1] Mayank Agrawal, et. al, "Industry 4.0: Reimagining Manufacturing Operations After COVID-19," McKinsey, July 29, 2020.

[2] "Global Threat Landscape Report, 1H 2021," Fortinet, August 2021.

[3] Clare Duffy, "Colonial Pipeline Attack: A 'Wake Up Call' about the Threat of Ransomware," CNN, May 16, 2021; Liam Tung, "Ransomware: Meat Firm JBS Says It Paid Out $11m After Attack," ZDnet, June 10, 2021.

[4] "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure," CISA, April 20, 2022.

[5] Catherine Stupp, "Russian Cyberattacks Increase on Ukraine's Critical Infrastructure: Report," Wall Street Journal, April 5, 2022.

[6] Phil Muncaster, "Critical Infrastructure Firms See Cyber-Attacks Surge," InfoSecurity, May 10, 2022.

[7] Steven Webb, "IT/OT & OT Total Available Market Analysis," Westlands Advisory Research for Fortinet, March 2022.

[8] "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure," CISA, April 20, 2022.

FORTINET

www.fortinet.com

Copyright © 2022 Fortinet, Inc. Todos os direitos reservados. Fortinet®, FortiGate®, FortiCare®, FortiGuard® e algumas outras marcas são marcas registradas da Fortinet, Inc. Outros nomes Fortinet mencionados neste documento também podem ser marcas registradas e/ou de direito consuetudinário da Fortinet. Todos os outros nomes de produtos ou de empresas podem ser marcas registradas de seus respectivos proprietários. O desempenho e outras métricas mencionados neste documento foram obtidos em testes laboratoriais internos sob condições ideais; o desempenho efetivo e outros resultados podem variar. As variáveis de rede, diferentes ambientes de rede e outras condições podem afetar os resultados de desempenho. Nada neste documento representa qualquer compromisso vinculante da Fortinet, e a Fortinet renuncia a todas as garantias, expressas ou implícitas, exceto na medida em que a Fortinet celebre um contrato vinculante por escrito, assinado pelo conselho geral da Fortinet, com um comprador que garanta expressamente que o produto identificado operará de acordo com determinadas métricas de desempenho expressamente identificadas e, nesse caso, apenas as métricas de desempenho específicas identificadas expressamente em tal contrato de vinculação por escrito serão vinculativas à Fortinet. Para clareza absoluta, qualquer garantia deste tipo será limitada ao desempenho nas mesmas condições ideais dos testes laboratoriais internos da Fortinet. A Fortinet renuncia por completo a quaisquer convênios, representações e garantias nos termos do presente regulamento, expressos ou implícitos. A Fortinet reserva-se o direito de alterar, modificar, transferir ou revisar esta publicação sem aviso prévio, e a versão atual da publicação será aplicável.

julho 4, 2022 11:30 AM

1578659-0-0-PT