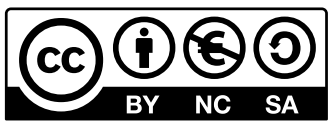
A Segurança da Infraestrutura Crítica na América Latina: Política, Risco e Resiliência

DIGI AMERICAS

DIGI AMERICAS ALLIANCE MEMBERS

aws Apple Batuta CHECK POINT CISCO CLOUDFLARE CROWDSTRIKE fluid attacks
Google kriptos LUMU netskope paloalto NETWORKS Resecurity
Schneider Electric SISAP Sistemas Aplicativos SOPHOS tenable Trellix TrendAI whalemate



Créditos

Digi Americas Alliance

Alain Karioty
Andy Kotz
Belisario Contreras
Brett DeWitt
Carlos Torales
Christian Torres
Cory Bullock
Federico Nan
Fernando Quintero
Gene Yoo
Ghassan Dreibi
Hernan Armbruster
Jordana Siegel
Jorge Blanco
Marcos Pupo
Mario de la Cruz Sarabia
Mauricio Nanne
Norberto (Bert) Milan
Patrick Ford
Rafael Alvarez
Ricardo Villadiego
Stephen Fallas

Editores

Belisario Contreras
Andy Kotz

Conteúdo

Introdução

Infraestrutura crítica (IC) refere-se a diversos setores e atores que sustentam a estabilidade nacional e o bem-estar público. Nos Estados Unidos, a Agência de Segurança de Cibersegurança e Infraestrutura (CISA) identifica 16 setores críticos de infraestrutura, incluindo Energia, Comunicações, Serviços Financeiros, Saúde e Saúde Pública, Transporte, Água e Esgoto, e Tecnologia da Informação, entre outros.[1] Embora as classificações variem entre países, os governos latino-americanos também reconhecem redes energéticas, redes de telecomunicações, sistemas financeiros, corredores de transporte, sistemas hídricos e serviços públicos como fundamentais para o crescimento econômico, governança democrática e estabilidade social.[2]

Nos últimos anos, esses sistemas têm se tornado cada vez mais alvos de operações cibernéticas maliciosas realizadas por grupos criminosos, hacktivistas, ameaças internas e atores patrocinados pelo Estado. Atores patrocinados pelo Estado, especialmente da China e da Rússia, tratam infraestrutura crítica não apenas como ativos econômicos, mas como alavanca estratégica na competição geopolítica.[3] Operações russas na Ucrânia mostram que ataques cibernéticos a redes governamentais, sistemas de telecomunicações e infraestrutura energética podem preceder ou acompanhar ações militares, o que borra a linha entre guerra cibernética e cinética.[4] De forma semelhante, campanhas ligadas à China, como Volt Typhoon e Salt Typhoon, têm como alvo setores de telecomunicações e outras infraestruturas críticas para obter acesso persistente e furtivo às redes — muitas vezes pré-posicionando-se dentro dos sistemas para possibilitar possíveis interrupções durante futuras crises geopolíticas.[5]

Para a América Latina, as apostas continuam particularmente altas. A região está passando por uma rápida transformação digital, expandindo a conectividade, modernizando a infraestrutura energética e integrando-se mais profundamente às cadeias de suprimentos globais. Ao mesmo tempo, muitos países enfrentam estruturas regulatórias desiguais, recursos limitados de cibersegurança, infraestrutura legada e crescente exposição a ameaças cibernéticas transnacionais. Esses riscos são agravados pelo aumento da atividade de grupos de ameaça avançada persistente (APT) ligados a grandes potências, que demonstraram a capacidade de infiltrar-se e persistir em redes de infraestrutura por longos períodos, muitas vezes sem serem detectados.[6] Como resultado, a segurança da infraestrutura crítica vai além de uma questão técnica; ela está no centro

[1] https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors
[2] https://blogs.worldbank.org/en/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe
[3] https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors
[4] https://www.atlanticcouncil.org/blogs/ukrainealert/learning-the-lessons-from-ukraines-fight-against-russian-cyber-warfare/
[5] https://www.congress.gov/crs-product/IF12798
[6] https://www.congress.gov/crs-product/IF12798

da resiliência nacional, da estabilidade regional e do desenvolvimento de longo prazo.[7]

Como a IC abrange setores diversos, nenhuma abordagem única pode garanti-la. Proteger um sistema de saúde requer medidas diferentes daquelas para proteger uma usina hidrelétrica ou um porto importante. Um fator chave que distingue a segurança de CI da cibersegurança tradicional está no uso da tecnologia operacional (OT), o hardware e software que monitoram e controlam processos físicos. Sistemas de controle industrial (ICS), que conectam sistemas de tecnologia da informação (TI) a ambientes de OT, criam riscos que diferem significativamente das redes convencionais de TI. Na maioria dos países, esses sistemas ainda dependem de tecnologias legadas originalmente projetadas para confiabilidade e continuidade operacional, em vez de cibersegurança.[8] Ao mesmo tempo, a IA agora remodela tanto a defesa quanto o ataque: defensores usam detecção de anomalias impulsionada por IA para identificar interrupções sutis em processos industriais, enquanto adversários podem usar IA para mapear redes complexas, descobrir vulnerabilidades em sistemas legados e criar estratégias de intrusão automatizadas e mais precisas contra ambientes OT.[9]

Historicamente, esses sistemas operavam em relativo isolamento e enfrentavam exposição limitada a ameaças cibernéticas.[10] No entanto, à medida que operadores de infraestrutura em toda a região adotam ferramentas digitais de monitoramento, recursos de acesso remoto e plataformas de gerenciamento baseadas em nuvem, os sistemas físicos tornaram-se mais interconectados e vulneráveis. A convergência dos ambientes de TI e OT expandiu a superfície de ataque para infraestrutura crítica nos setores de energia, água, mineração, transporte e telecomunicações. Essa superfície de ataque ampliada reflete vulnerabilidades exploradas na Ucrânia, onde atores russos têm mirado repetidamente redes elétricas, redes de comunicação e serviços digitais com campanhas cibernéticas cada vez mais sofisticadas desde 2014.[11] A IA acelera essa situação porque permite ataques mais escaláveis e adaptativos, ao mesmo tempo em que capacita defensores a implantar análises preditivas, resposta automatizada a incidentes e gêmeos digitais para simular e mitigar falhas em cascata em sistemas interconectados.

Em todos os setores, as cadeias de suprimentos representam um alvo especialmente atraente para atores maliciosos. Ao comprometer fornecedores, provedores de serviços gerenciados ou dependências de software, adversários podem obter acesso indireto a ativos de infraestrutura de alto valor. Esses riscos não são teóricos. No caso do Volt Typhoon, ligado à China, agências de inteligência alertaram que atacantes infiltraram setores como energia, transporte e sistemas hídricos e mantiveram o acesso por

[7] https://blogs.worldbank.org/en/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe
[8] https://www.cisa.gov/topics/industrial-control-systems
[9] https://red.anthropic.com/2026/mythos-preview/
[10] https://www.cisa.gov/topics/industrial-control-systems
[11] https://www.atlanticcouncil.org/blogs/ukrainealert/learning-the-lessons-from-ukraines-fight-against-russian-cyber-warfare/

anos, sugerindo uma estratégia focada em pré-posicionamento para possíveis interrupções em crises futuras, em vez da espionagem tradicional.[12]

Governos, reguladores, proprietários e operadores de CI, e parceiros do setor privado em toda a América Latina, portanto, precisam se adaptar a um cenário de ameaças em evolução. Ao fazer isso, é importante distinguir os papéis dos atores dentro desse ecossistema: operadores de infraestrutura crítica têm responsabilidade direta pela segurança dos sistemas que operam, enquanto provedores de tecnologia, incluindo provedores de serviços em nuvem, desenvolvedores de software e fabricantes de equipamentos, apoiam essa missão com plataformas seguras, certificadas e transparência sobre a segurança de seus produtos. Nesse contexto, a IA deve ser entendida não como uma solução independente, mas como um multiplicador de força: seu uso eficaz dependerá de estruturas de governança, qualidade dos dados e expertise humana, enquanto seu uso indevido pode reduzir a barreira de entrada para operações cibernéticas sofisticadas contra infraestruturas críticas. Enfrentar os riscos de convergência de TI/OT, fortalecer a segurança da cadeia de suprimentos com obrigações adequadas ao cargo, investir diretamente no desenvolvimento da força de trabalho e adotar princípios de secure-by-design e secure-by-default são passos críticos para construir uma infraestrutura mais resiliente em toda a região.

[12] https://www.theguardian.com/technology/2024/feb/08/chinese-hack-us-transportation-infrastructure

Identificação e Priorização de Infraestrutura Crítica

Identificar e priorizar corretamente infraestrutura crítica é um passo fundamental para desenvolver estratégias eficazes de cibersegurança, especialmente em ambientes com recursos limitados. Os governos devem primeiro determinar quais ativos e sistemas são mais essenciais para a segurança nacional, estabilidade econômica e segurança pública, já que nem toda infraestrutura pode ser protegida igualmente. Esse processo normalmente envolve avaliações baseadas em riscos que avaliam tanto a probabilidade de interrupção quanto as possíveis consequências de falhas, incluindo efeitos de transbordamento em setores interconectados. Nesse contexto, os governos também devem considerar ativos menos visíveis, mas altamente consequentes. Esses podem incluir cabos de telecomunicações submarinos, que transportam a maior parte do tráfego internacional de dados e são críticos para a continuidade econômica e a conectividade nacional. Apesar de sua importância, esses ativos são frequentemente negligenciados nos frameworks tradicionais de infraestrutura crítica e podem carecer de medidas adequadas de proteção física e cibernética.

Na América Latina, onde as dependências entre energia, telecomunicações, sistemas financeiros e redes de transporte estão aumentando, a priorização também deve levar em conta o risco sistêmico e as interdependências intersetoriais. Cenários que introduzem ambientes híbridos de risco onde ameaças físicas e cibernéticas convergem, como sistemas aéreos não tripulados (drones) sendo usados para atingir infraestrutura física, exigem definições ampliadas do que constitui infraestrutura crítica.

Ao definir ativos críticos e classificá-los de acordo com sua importância estratégica e vulnerabilidade, formuladores de políticas e operadores podem alocar recursos limitados de forma mais eficaz, focar esforços de mitigação e melhorar a resiliência geral contra ameaças cibernéticas e físicas. Além disso, setores como serviços espaciais (incluindo comunicações via satélite e GPS), data centers que suportam infraestrutura em nuvem e oleodutos de energia submarina deveriam ser mais bem incorporados aos inventários nacionais de infraestrutura crítica, pois sua interrupção pode ter impactos desproporcionais e transfronteiriços.

Segurança da Cadeia de Suprimentos

Cadeias de suprimentos de infraestrutura crítica são ecossistemas complexos que podem abranger centenas de fornecedores, integradores, proprietários, operadores e prestadores de serviços.[13] Eles incluem fabricantes de hardware, desenvolvedores de software, provedores de nuvem, contratados de manutenção,

[13] https://www.energy.gov/ceser/supply-chain-cybersecurity-principles

empresas de logística, órgãos de certificação e autoridades regulatórias. Essas cadeias de suprimentos interagem por meio de processos físicos como produção e transporte, bem como por serviços digitais como monitoramento remoto, atualizações de software e troca de dados.[14]

Um dos desenvolvimentos mais significativos que afetam infraestrutura crítica e suas cadeias de suprimentos é a rápida digitalização.[15] Sistemas de infraestrutura estão cada vez mais dependentes de componentes orientados por software, serviços baseados em nuvem e conectividade remota. A IA transforma ainda mais as cadeias de suprimentos porque possibilita manutenção preditiva, tomada de decisão automatizada e análises em tempo real, além de introduzir novos riscos relacionados à integridade dos dados, segurança do modelo e manipulação adversarial. Olhando para o futuro, os avanços na computação quântica podem desafiar os padrões criptográficos atuais que sustentam comunicações seguras entre cadeias de suprimentos, o que cria a necessidade de planejamento de longo prazo em torno da criptografia resistente à quântica. Como resultado, a segurança de um único operador agora depende da resiliência de cada elo em sua cadeia de suprimentos. Uma vulnerabilidade introduzida por um fornecedor externo de software, provedor de serviços gerenciados ou fornecedor de equipamentos pode se espalhar por múltiplos setores e até mesmo além de fronteiras nacionais.

Para gerenciar a complexidade crescente, as organizações podem iniciar uma redução significativa de riscos com o estabelecimento e aplicação de padrões mínimos de cibersegurança para fornecedores. O que distingue a cibersegurança da cadeia de suprimentos no contexto da IC é sua natureza coletiva e o fato de que diferentes atores carregam obrigações distintas e claramente definidas. Os operadores de infraestrutura crítica mantêm a responsabilidade principal pela segurança de seus ambientes operacionais, incluindo como configuram, integram e governam tecnologias de terceiros nesses ambientes. Provedores de tecnologia como provedores de serviços em nuvem, provedores de serviços de segurança gerenciada e fornecedores de software são responsáveis pela segurança de suas plataformas e serviços, tipicamente evidenciada por certificações do setor (ISO 27001, SOC 2, equivalente ao FedRAMP), compromissos contratuais e políticas publicadas de responsabilidade compartilhada. Requisitos de segurança de linha básica claros, mecanismos contratuais de fiscalização e supervisão adequada devem refletir essa diferenciação de funções — garantindo responsabilidade em todas as etapas da compra, integração e manutenção sem transferir a responsabilidade do operador para provedores que não controlam como seus serviços são implementados.

A distribuição dessas obrigações de visibilidade deve seguir o controle operacional: os operadores de infraestrutura são responsáveis por

[14] https://www.nics.uma.es/wp-content/papers/Roman2023a.pdf
[15] https://www.nics.uma.es/wp-content/papers/Roman2023a.pdf

inventariar suas próprias implantações, configurações e dependências, incluindo quaisquer componentes baseados na nuvem. Os provedores de tecnologia, por sua vez, são responsáveis por fornecer a documentação — listas de materiais de software, avisos de segurança, detalhes claros da arquitetura e evidências de auditoria — que permitem aos operadores cumprir suas próprias obrigações de visibilidade. À medida que as cadeias de suprimentos se expandem para incluir serviços impulsionados por IA e, no futuro, capacidades habilitadas por quântico, a transparência em torno de algoritmos, fontes de dados e dependências criptográficas se tornará mais crítica. Estruturas regulatórias que exigem que os provedores realizem exercícios de visibilidade nos ambientes do cliente invertem essa lógica e minam a responsabilidade efetiva.

Monitoramento contínuo, avaliações de riscos por terceiros e cláusulas de cibersegurança embutidas nos contratos de aquisição traduzem compromissos políticos de alto nível em prática operacional. Secure-by-design e secure-by-default devem se tornar requisitos de aquisição, não apenas aspirações. As organizações devem incorporar os requisitos de cibersegurança nos contratos com fornecedores com critérios mensuráveis de conformidade e estabelecer uma responsabilidade clara. Isso inclui a exigência de que os fornecedores demonstrem práticas seguras de desenvolvimento para sistemas de IA e planejamento antecipado para a prontidão pós-quântica da criptografia. Para tornar essas linhas de base eficazes em larga escala, governos e consórcios industriais devem se alinhar em estruturas padronizadas e políticas de compras. Iniciativas como o Quadro de Cibersegurança 2.0 do NIST[16] e os princípios de segurança desde o design[17] da CISA podem servir como modelos fundamentais para harmonizar as expectativas dos fornecedores e garantir a responsabilização. À medida que a transformação digital acelera, a superfície de ataque da infraestrutura crítica só irá se expandir. Portanto, fortalecer a segurança da cadeia de suprimentos não é apenas uma necessidade técnica, mas um imperativo estratégico para a resiliência nacional e a estabilidade econômica.

Convergência OT/TI e suas implicações para a segurança

À medida que a integração entre TI e OT aumenta, suas medidas de segurança não devem funcionar como sistemas isolados. A segurança tradicional de TI enfatiza a tríade confidencialidade, integridade e disponibilidade (CIA), enquanto a segurança OT prioriza a operação contínua e confiável dos processos físicos e dos sistemas de controle. Para se proteger contra uma gama crescente de ameaças cibernéticas, os ambientes OT dependem de sistemas de controle de supervisão e aquisição de dados (SCADA) e sistemas de

[16] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
[17] https://www.cisa.gov/securebydesign

controle industrial para manter a resiliência operacional.[18] A contínua convergência de TI e OT apresenta um desafio: alinhar as diferentes prioridades desses domínios para garantir tanto a resiliência cibernética quanto o desempenho operacional ininterrupto em toda a cadeia de suprimentos da infraestrutura crítica.

Tecnologias emergentes e emergentes aceleram essa convergência. A IA aprimora a detecção de ameaças, automatiza a identificação de anomalias e otimiza a eficiência operacional tanto em ambientes de TI quanto OT. No entanto, essas capacidades também introduzem novos riscos, incluindo o potencial de ataques adversariais a modelos de IA, envenenamento de dados e dependência excessiva de decisões automatizadas em sistemas críticos para a segurança. Ao mesmo tempo, o impacto futuro da computação quântica e de outras tecnologias emergentes na criptografia e comunicações seguras representa um desafio estratégico para sistemas de TI e OT, especialmente onde ativos de infraestrutura de longa duração dependem de proteções criptográficas que podem se tornar vulneráveis com o tempo. A preparação para essas mudanças exigirá estratégias de segurança práticas e voltadas para o futuro que incorporem governança de IA e criptografia resiliente à quantum.

Além dos resultados técnicos, os procedimentos de resposta a ameaças e as obrigações de conformidade para TI e OT frequentemente diferem na prática. Governos e reguladores devem levar em conta essas distinções ao elaborarem requisitos futuros e devem distinguir ainda mais entre operadores e integradores de infraestrutura crítica — que têm responsabilidade operacional direta — e provedores de soluções tecnológicas, como plataformas em nuvem ou serviços de conectividade, cujas obrigações regulatórias devem estar alinhadas com sua esfera real de controle. Aplicar obrigações de operadores de infraestrutura crítica a provedores de tecnologia que não operam diretamente sistemas essenciais distorceria a responsabilidade e arriscaria retardar a adoção de capacidades avançadas de segurança que operadores com recursos limitados urgentemente precisam.

Pesquisa de Especialistas Regionais

Contexto

Para compreender melhor o ecossistema de cibersegurança de infraestrutura crítica na América Latina, a Digi Americas Alliance realizou uma pesquisa com 141 partes interessadas em toda a região. Aproximadamente 46% dos entrevistados trabalham em operadores de infraestrutura crítica, enquanto os demais representam organizações relacionadas envolvidas em cibersegurança, tecnologia e políticas públicas. Os entrevistados representam um conjunto diversificado de países, incluindo Colômbia (19%), México (14%), Argentina (9%), Panamá (7%) e Equador (7%), além de Brasil, Costa Rica, Espanha,

[18] https://www.paloaltonetworks.com/cyberpedia/iot-security-vs-ot-security

Uruguai, República Dominicana, Chile, Estados Unidos, Venezuela, Guatemala, Honduras, Paraguai e Peru.

Os participantes também representam diversos papéis dentro de suas organizações. Quase metade dos entrevistados (47%) trabalha em cargos relacionados à segurança, enquanto 21% são membros da alta direção. Outros 19% trabalham em funções tecnológicas mais amplas, com os demais respondentes atuando em áreas como cibersegurança, gestão geral, análise e vendas. Essa diversidade de funções mostra como diferentes grupos interpretam os desafios de cibersegurança como percebidos entre a liderança organizacional, equipes técnicas e partes interessadas operacionais.

Organizações

Os entrevistados representam organizações com diferentes estruturas de propriedade que atuam em múltiplos setores. Aproximadamente 60% trabalham em organizações privadas, 30% em organizações públicas ou governamentais, e 10% em organizações com estruturas de propriedade mistas.

As organizações pesquisadas também abrangem uma ampla gama de setores que desempenham papéis-chave nas economias nacionais e nos serviços públicos. A maior parcela dos entrevistados trabalha no setor de tecnologia da informação (24%), seguida por serviços financeiros (19%) e serviços governamentais (11%). Outros setores representados incluem energia (8%), comunicações, educação, saúde e saúde pública, agricultura e várias outras indústrias. Essa diversidade mostra que a infraestrutura crítica abrange múltiplos setores e que os riscos podem se mover de um setor para outro.

Resultados da Pesquisa

Fig. 1 — Sua organização possui uma estratégia de cibersegurança documentada?

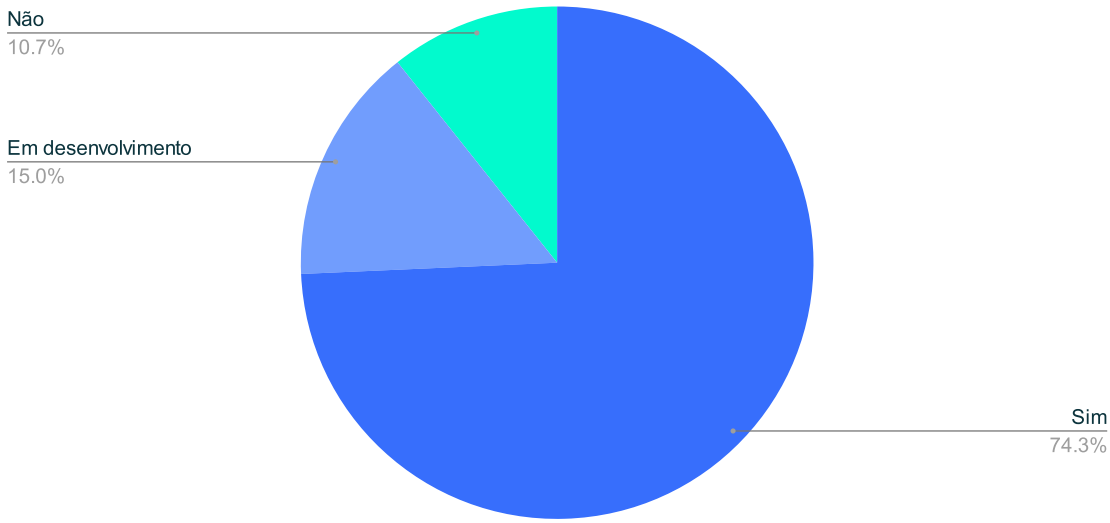


Fig. 2 — Sua organização possui uma estratégia dedicada à OT ou inclui OT em sua estratégia de cibersegurança?

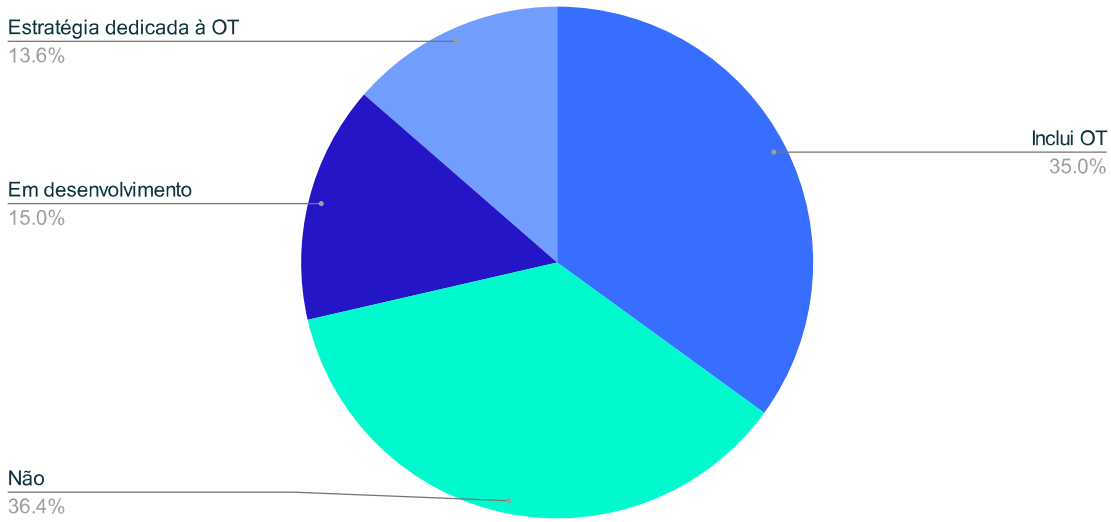


Fig. 3 — Sua organização depende de práticas de segurança de TI para proteger ambientes OT?

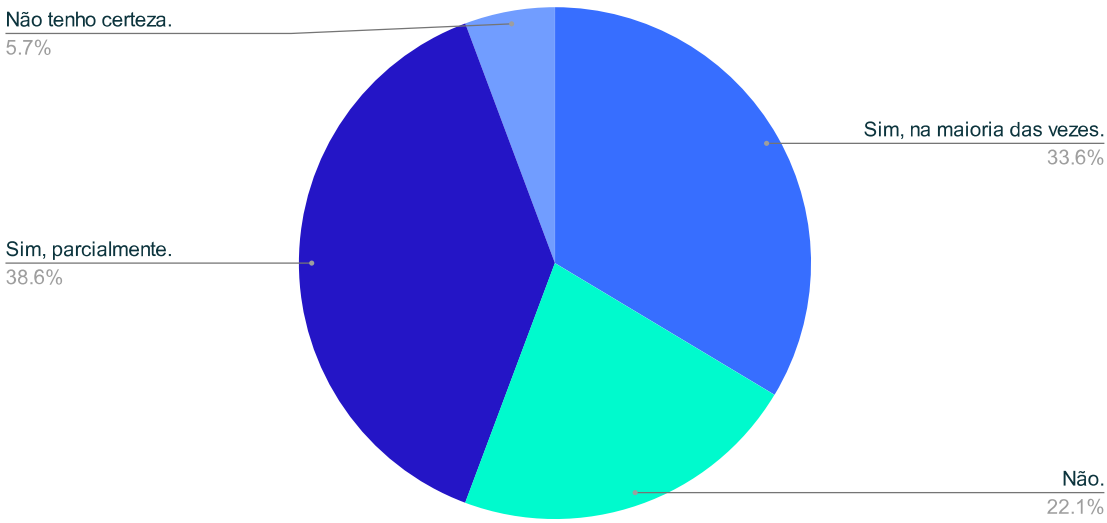
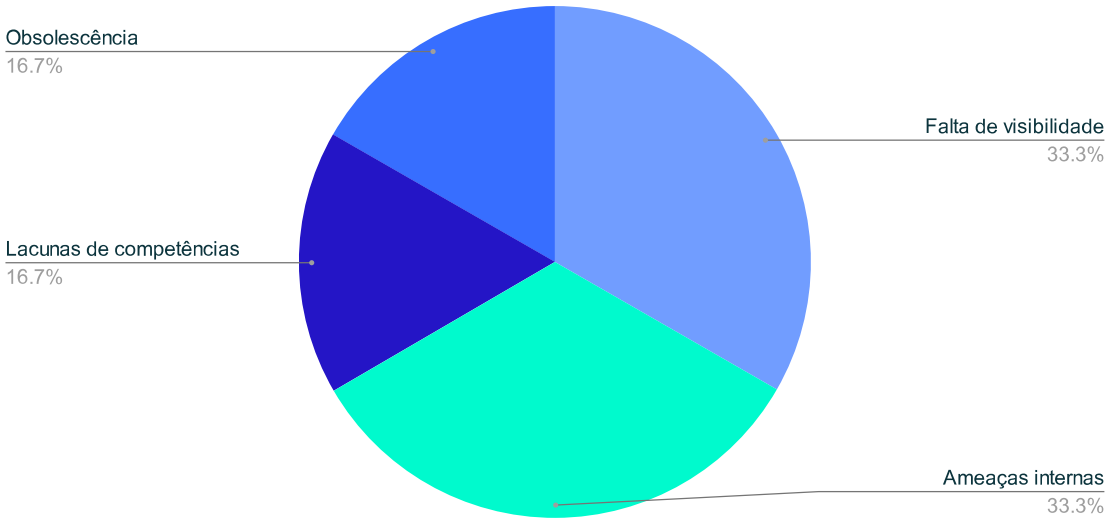


Fig. 4 — Quais são seus principais desafios para proteger dados sensíveis e regulamentados em TI/OT?



Um dos passos mais importantes para as organizações, especialmente aquelas designadas como infraestrutura crítica, é estabelecer um plano claro para proteger tanto seus ativos operacionais de tecnologia quanto de tecnologia da informação (TI). A Figura 1 mostra que a maioria das organizações (90%) possui uma estratégia de cibersegurança documentada ou está desenvolvendo uma ativamente. No entanto, a Figura 2 indica que a maioria (51%) dessas mesmas organizações atualmente não possui um plano que faça uma referência explícita à OT, o que aponta para uma lacuna crítica que precisa ser abordada. Proteger sistemas físicos exige planos deliberados que abordem os riscos distintos associados aos ambientes de TO. A Figura 3 destaca ainda mais que a maioria das organizações (72%) depende pelo menos parcialmente das práticas de segurança de TI para proteger os sistemas OT. Embora TI e OT compartilhem algumas semelhanças, envolvem requisitos operacionais e perfis de risco fundamentalmente diferentes e, portanto, exigem estratégias e práticas de segurança distintas.

IA na Segurança

Fig. 5 — Sua organização está utilizando atualmente IA ou aprendizado de máquina para fins de cibersegurança?

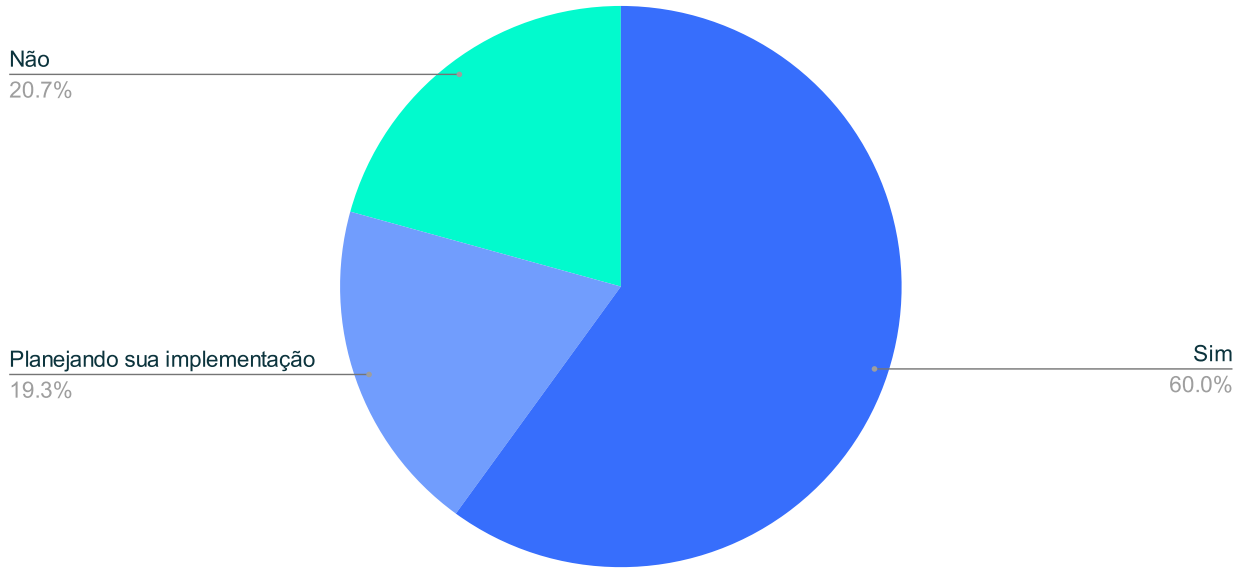


Fig. 6 — Sua organização desenvolveu e aplicou políticas de uso de IA para uso interno e fornecedores?

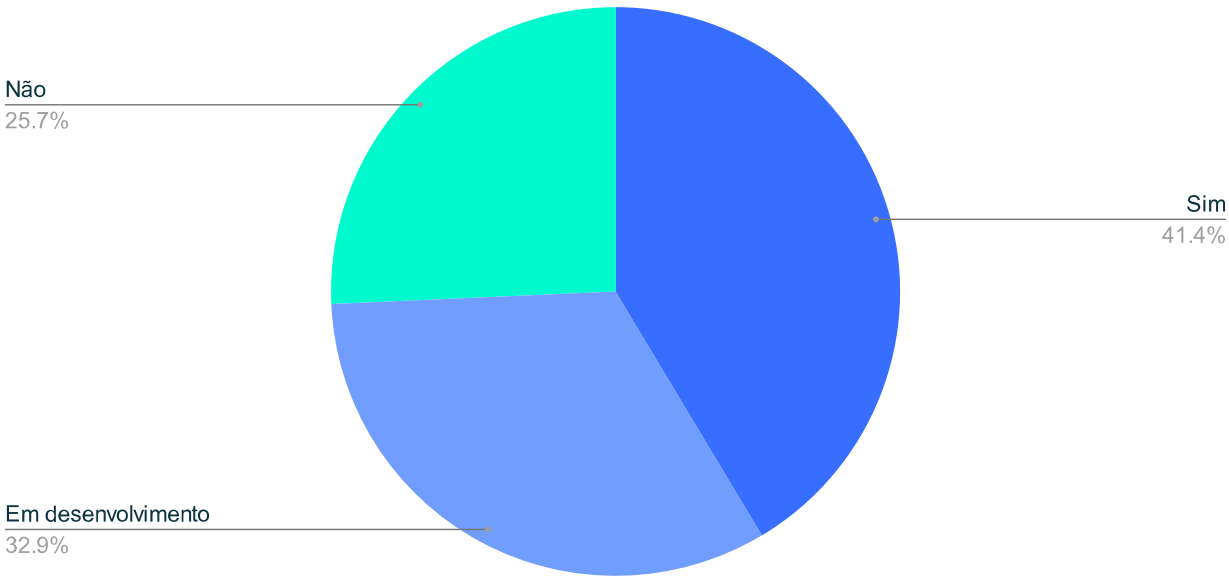


Fig. 7 — O quão preparada sua organização se considera para enfrentar ameaças cibernéticas impulsionadas por IA?

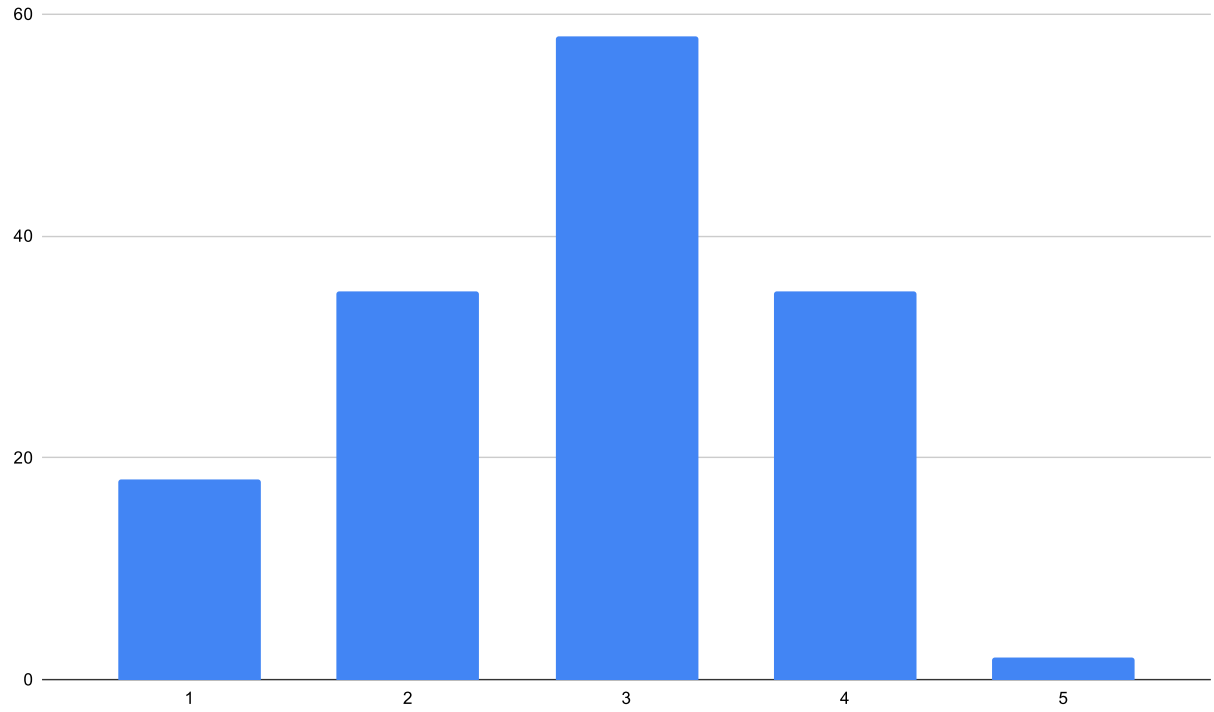
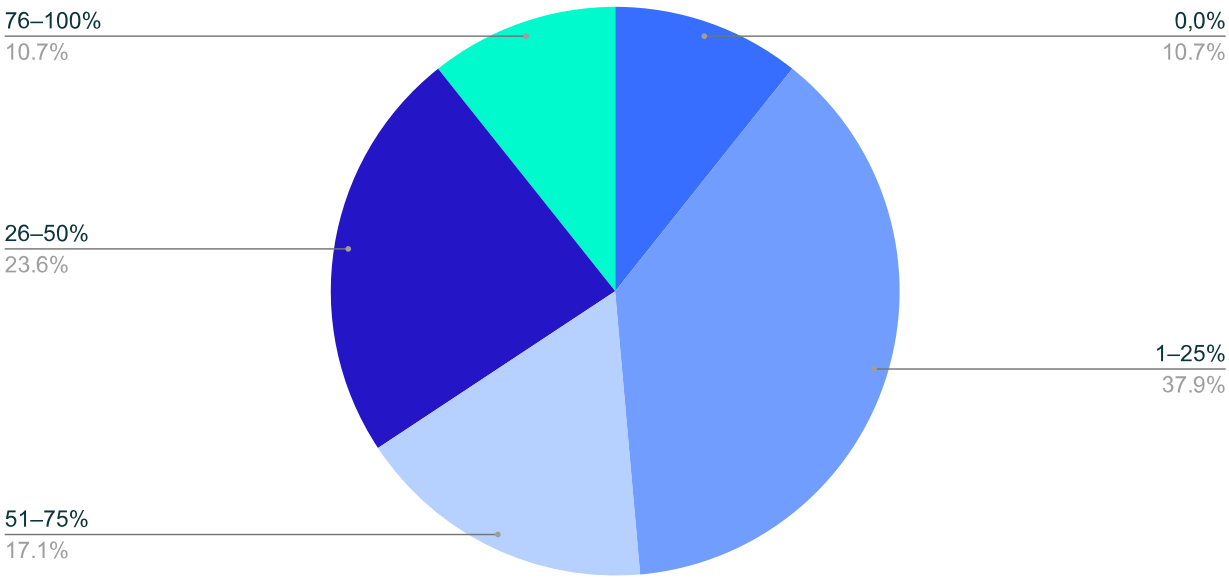


Fig. 8 — Qual porcentagem de seus sistemas críticos (TI/OT) funciona atualmente em infraestrutura na nuvem?



As Figuras 5 e 6 destacam o papel crescente da inteligência artificial nas operações de cibersegurança dentro de organizações de infraestrutura crítica. Aproximadamente 80% dos entrevistados relataram que suas organizações utilizam ativamente IA em sistemas de cibersegurança (60%) ou estão planejando sua implementação (19%). Isso sugere que a IA já está tendo um impacto significativo nas operações de cibersegurança, especialmente em áreas como detecção, monitoramento e automação de ameaças. No entanto, apesar dessa adoção generalizada, cerca de 25% das organizações relatam não possuir uma política formal de IA que regule o uso interno ou provedores terceirizados. À medida que a IA continua a evoluir e se integrar mais aos ambientes de cibersegurança, estabelecer políticas claras será essencial para gerenciar tanto os benefícios quanto os riscos potenciais associados ao seu uso.

A Figura 7 destaca o outro lado do papel crescente da IA na cibersegurança: o surgimento de ameaças novas e mais sofisticadas. A IA introduz tanto capacidades defensivas quanto novos vetores de ataque. Portanto, as organizações devem abordar a segurança da IA em três dimensões: IA para segurança (usando IA para detectar anomalias e automatizar resposta a ameaças), segurança para IA (para proteger sistemas de IA contra ataques adversariais) e governança da IA (para estabelecer políticas para uso responsável da IA). Quando questionados sobre o quão preparada sua organização está para lidar com ameaças cibernéticas impulsionadas por IA, como deepfakes ou malwares gerados por IA, quase nenhum entrevistado indicou se sentir "muito preparado". A maioria dos entrevistados selecionou um nível moderado de preparação (3), e muitos outros optaram por níveis mais baixos (2) ou um pouco maiores (4). Essas respostas mostram que, embora as organizações estejam adotando cada vez mais a IA como ferramenta defensiva, muitas ainda se sentem inseguras quanto à sua capacidade de combater ataques habilitados por IA. Como as capacidades de IA continuam avançando, é crucial melhorar a prontidão organizacional para enfrentar essas ameaças, que se tornarão cada vez mais importantes.

Segurança em Nuvem

A infraestrutura em nuvem oferece vantagens críticas que protegem melhor a tecnologia operacional e os sistemas de infraestrutura crítica do que ambientes locais podem igualar. Para organizações latino-americanas com recursos limitados que enfrentam ameaças sofisticadas patrocinadas pelo Estado, a adoção da nuvem transforma a cibersegurança de um fardo caro que exige investimento constante em uma capacidade compartilhada que melhora com a escala. Isso a torna mais segura como imperativo estratégico para proteger infraestruturas críticas, ao mesmo tempo em que possibilita a transformação digital.

A Figura 8 destaca até que ponto sistemas críticos de infraestrutura atualmente operam em ambientes em nuvem. Os resultados mostram que a maioria das organizações começou a integrar tecnologias em nuvem em suas operações, embora tipicamente de forma limitada. A maior parcela dos entrevistados (37,9%) relatou que entre 1 e 25% de seus sistemas críticos (TI/OT) atualmente operam na

nuvem. Outros 23,6% indicaram que entre 26 e 50% de seus sistemas operam em ambientes em nuvem, enquanto porções menores relataram níveis mais altos de adoção, incluindo 17,1% com 51–75% dos sistemas na nuvem e 10,7% com 76–100%. Apenas uma pequena parcela dos entrevistados relatou não usar a nuvem ou adoção muito mínima.

Esses resultados sugerem que, embora as tecnologias em nuvem migrem para ambientes de infraestrutura crítica, muitas organizações ainda adotam uma abordagem cautelosa, especialmente para sistemas operacionais de tecnologia que tradicionalmente permaneceram on-premises. À medida que a adoção da nuvem se expande, as organizações devem garantir que controles de segurança apropriados, a visibilidade e os frameworks de governança protejam os ativos de TI e OT em ambientes híbridos e baseados em nuvem.

Melhores Práticas

Os resultados da pesquisa indicam que governos, indústria e outros atores devem agir. Embora muitos países da região ainda estejam desenvolvendo políticas e marcos regulatórios para lidar com a segurança da infraestrutura crítica, vários governos e instituições ao redor do mundo já começaram a implementar estratégias, padrões e orientações voltados para fortalecer a resiliência da infraestrutura crítica e dos sistemas industriais. Esses esforços demonstram uma variedade de abordagens, incluindo a integração da segurança de OT às estratégias nacionais de cibersegurança, o desenvolvimento de estruturas dedicadas de OT, o fortalecimento da segurança da cadeia de suprimentos e o estabelecimento de requisitos regulatórios regionais para setores críticos.

A seção a seguir destaca uma seleção dessas melhores práticas, tanto dentro quanto fora da região. Ao apresentar iniciativas existentes, a seção visa fornecer a formuladores de políticas, reguladores e operadores do setor privado exemplos práticos de como governos e organizações estão lidando com riscos críticos de cibersegurança. Esses modelos oferecem lições que podem ajudar os países a desenvolver ou aprimorar seus próprios frameworks, promover uma colaboração público-privada mais forte e estabelecer padrões consistentes para proteger os sistemas que sustentam os serviços essenciais e a infraestrutura crítica.

Brasil

Estratégia Nacional de Cibersegurança

A Estratégia Nacional de Cibersegurança do Brasil (E-Ciber) enfatiza a proteção da infraestrutura crítica e dos serviços essenciais, como energia, telecomunicações, saúde e outros setores estratégicos, que dependem fortemente dos sistemas OT.[19] A estratégia prioriza a melhoria da segurança e resiliência da infraestrutura crítica, promovendo a gestão de riscos, prevenção de incidentes e uma coordenação mais forte entre governo e setor privado para prevenir e responder a incidentes cibernéticos que afetam esses sistemas.

[19] https://www.in.gov.br/en/web/dou/-/decreto-n-12.573-de-4-de-agosto-de-2025-646200784

Ao vincular explicitamente a política de cibersegurança à proteção de serviços e infraestrutura essenciais, a estratégia do Brasil também aborda a segurança dos ambientes de OT que sustentam esses setores. Essa abordagem oferece uma lição útil para outros países da região e demonstra que as estratégias nacionais de cibersegurança não devem focar apenas em sistemas de TI, mas também incorporar a proteção de sistemas industriais e operacionais que apoiam infraestrutura crítica. Incorporar a segurança da OT em estruturas nacionais mais amplas de governança cibernética pode ajudar os governos a fortalecer a resiliência, incentivar a colaboração público-privada e promover padrões de segurança consistentes em setores críticos.

Colômbia

Estratégia Nacional de Segurança Digital 2025-2027

A Estratégia Nacional de Segurança Digital da Colômbia 2025–2027 baseia-se na base estabelecida pela CONPES 3995 (2020) e adota uma abordagem mais operacional e focada na implementação para a cibersegurança, com forte ênfase na proteção de infraestruturas críticas e serviços essenciais.[20] [21] A estratégia prioriza a segurança e a resiliência da infraestrutura cibernética crítica, reconhecendo seu papel central no apoio a setores como energia, finanças, saúde e serviços governamentais.

Um elemento-chave da estratégia é sua ênfase na resiliência cibernética e na gestão de riscos. Promove a identificação proativa de vulnerabilidades, monitoramento contínuo e capacidades mais fortes de detecção e resposta a incidentes, tanto em operadores públicos quanto privados. O quadro também enfatiza a preparação para incidentes cibernéticos em grande escala, incluindo mecanismos nacionais coordenados de resposta e melhores capacidades de recuperação para serviços essenciais. Além disso, a estratégia fortalece a governança institucional e o fortalecimento de capacidades, abordando lacunas identificadas em estruturas anteriores. Inclui esforços para aprimorar as capacidades nacionais de defesa cibernética, expandir o desenvolvimento da força de trabalho e alinhar iniciativas de cibersegurança com objetivos mais amplos de desenvolvimento nacional e transformação digital.

A abordagem da Colômbia oferece uma lição fundamental para a região: fortalecer a resiliência da infraestrutura crítica requer não apenas controles técnicos, mas também estruturas de governança bem definidas e capacidades nacionais coordenadas. A integração da cibersegurança em estruturas mais amplas de confiança digital e gestão de riscos pode melhorar a capacidade dos países de gerenciar melhor ameaças a ambientes de TI e operacionais que apoiam serviços essenciais.

[20] https://www.mintic.gov.co/portal/715/articles-403023_recurso_2.pdf
[21] https://depp.oecd.org/policies/COL2168

União Europeia

Diretiva 2022/2555 - NIS2

A Diretiva 2 da União Europeia sobre Segurança da Rede e da Informação (NIS2) estabelece uma das abordagens regulatórias mais abrangentes para a cibersegurança de infraestruturas críticas.[22] Adotada em 2022 e substituindo a Diretiva original do NIS, a NIS2 estabelece um arcabouço jurídico comum para cibersegurança entre os Estados-membros da UE, abrangendo organizações que atuam em 18 setores críticos como energia, transporte, saúde, finanças e infraestrutura digital. A diretriz obriga entidades públicas e privadas consideradas "essenciais" ou "importantes" a implementar medidas de gestão de riscos, melhorar a governança e as capacidades de resposta a incidentes, e reportar incidentes cibernéticos significativos às autoridades nacionais dentro de prazos definidos.[23]

A diretiva tem implicações claras para a tecnologia operacional e a infraestrutura ciberfísica, já que muitos setores cobertos dependem fortemente de sistemas de controle industrial e outros ambientes OT. Ao impor controles básicos de segurança, gestão de riscos na cadeia de suprimentos e responsabilidade executiva pela cibersegurança, o NIS2 melhora a resiliência geral da infraestrutura crítica em toda a UE.[24]

Esse modelo oferece uma lição útil para outras regiões: estabelecer requisitos harmonizados de cibersegurança para setores críticos em nível regional pode ajudar a padronizar proteções, melhorar a cooperação transfronteiriça e garantir que tanto os sistemas de TI quanto os OT que apoiam serviços essenciais estejam protegidos contra ameaças cibernéticas em evolução.

México

Plano Nacional de Cibersegurança 2025-2030

O Plano Nacional de Cibersegurança do México 2025–2030[25] marca uma mudança significativa em direção a um modelo de cibersegurança mais centralizado, preventivo e focado em infraestrutura. Desenvolvido pela Agência para a Transformação Digital e Telecomunicações (ATDT), o plano representa a primeira política abrangente e intersetorial de cibersegurança do país e prioriza a proteção da infraestrutura crítica e dos serviços essenciais como objetivo nacional central.[26]

Um componente central do plano é a criação de uma governança unificada e uma arquitetura operacional para substituir esforços historicamente fragmentados. Isso inclui o estabelecimento de um Centro Nacional de Operações de Cibersegurança (CNSOC) para monitoramento em tempo real, um centro federal de resposta

[22] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555
[23] https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
[24] https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
[25] https://www.gob.mx/atdt/comunicacion/liderara-mexico-ciberresiliencia-en-la-region-con-plan-nacional-de-ciberseguridad
[26] https://mexicobusiness.news/cybersecurity/news/mexico-unveils-national-cybersecurity-plan-2025-2030

a incidentes (CSIRT) e um inventário nacional de infraestrutura crítica para identificar e priorizar a proteção de ativos estratégicos em setores como energia, finanças, telecomunicações e sistemas governamentais.[27] Essas medidas são complementadas por um sistema de avaliação de vulnerabilidades e alerta projetado para identificar e remediar proativamente fraquezas nos sistemas do setor público.[28]

O plano também introduz padrões obrigatórios de cibersegurança, requisitos de reporte de incidentes e estruturas de gestão de riscos para entidades federais, o que sinaliza uma tendência para proteções mais aplicáveis e padronizadas para infraestrutura crítica. Paralelamente, o México busca fortalecer a coordenação entre governo, indústria e academia por meio de um Conselho Nacional de Cibersegurança e mecanismos ampliados de compartilhamento de informações, reconhecendo que a resiliência da infraestrutura depende da colaboração entre múltiplos interessados.[29]

A abordagem do México oferece uma lição importante para a região: a transição de esforços fragmentados em cibersegurança para um quadro centralizado e orientado por políticas — com instituições dedicadas, padrões obrigatórios e um inventário nacional de infraestrutura crítica — pode aumentar significativamente a visibilidade, coordenação e resiliência.

Ao mesmo tempo, o caso mexicano ressalta a necessidade de complementar reformas de governança de alto nível com orientações específicas de setores e técnicas, especialmente para ambientes de TO que sustentam infraestruturas críticas.

Singapura

Plano Diretor de Cibersegurança em Tecnologia Operacional 2024

Singapura adotou uma abordagem direcionada à segurança da tecnologia operacional (OT) por meio do seu Plano Mestre de Cibersegurança em Tecnologia Operacional 2024, lançado pela Agência de Cibersegurança de Singapura (CSA).[30] O plano atua como um plano nacional para fortalecer a postura de cibersegurança das organizações que operam sistemas de TO tanto em setores de infraestrutura crítica de informação (CII) quanto em outros setores dependentes de TO. Foca no fortalecimento das capacidades em três pilares (pessoas, processos e tecnologia), incluindo a expansão do pipeline de talentos em cibersegurança em OT, melhor compartilhamento de informações e relatos de incidentes, resiliência além dos setores tradicionais de infraestrutura crítica e o uso de princípios de segurança por implantação e segurança por design ao longo do ciclo de vida dos sistemas OT.[31]

[27] https://nearshoreamericas.com/mexico-moves-to-strengthen-cybersecurity-with-new-national-plan-and-law/
[28] https://blog.knowbe4.com/mexico-unveils-its-first-national-cybersecurity-plan-a-new-era-of-digital-resilience
[29] https://www.eleconomista.com.mx/tecnologia/gobierno-sheinbaum-presenta-plan-nacional-ciberseguridad-2025-20251204-789652.html
[30] https://www.csa.gov.sg/resources/publications/singapore-s-operational-technology-cybersecurity-masterplan-2024/
[31] https://www.csa.gov.sg/resources/publications/singapore-s-operational-technology-cybersecurity-

A abordagem de Singapura oferece uma lição importante para outras regiões: em vez de tratar a segurança de OT apenas como um subconjunto da política geral de cibersegurança, os governos podem desenvolver estruturas nacionais dedicadas para sistemas OT que abordem o desenvolvimento da força de trabalho, coordenação setorial e segurança ao longo do ciclo de vida das tecnologias industriais. Ao integrar agências governamentais, partes interessadas do setor e instituições educacionais em uma estratégia coordenada, Singapura demonstra como os países podem fortalecer proativamente a resiliência da infraestrutura crítica e dos sistemas físicos emergentes.[32]

Estados Unidos da América

Princípios de Cibersegurança da Cadeia de Suprimentos do Departamento de Energia (DOE)

Em 2024, o Departamento de Energia dos EUA (DOE) para Cybersegurança, Segurança Energética e Resposta a Emergências (CESER) divulgou um conjunto de princípios de cibersegurança da cadeia de suprimentos para apoiar fornecedores e usuários finais, a fim de proteger a cadeia de suprimentos, com foco específico no setor de energia.[33] Os princípios abrangiam os seguintes conceitos e objetivos de cibersegurança:

- Gestão de riscos orientada por impacto
- Defesas informadas por estrutura
- Fundamentos da cibersegurança
- Desenvolvimento e implementação seguros
- Transparência e construção de confiança
- Orientação de implementação
- Suporte e manutenção ao ciclo de vida
- Gerenciamento proativo de vulnerabilidades
- Resposta proativa a incidentes
- Resiliência nos negócios e operacionalmente

O documento também enfatiza que a segurança é uma responsabilidade compartilhada e que a colaboração é absolutamente necessária em uma cadeia de suprimentos complexa. Por exemplo, o documento destaca que "Fornecedores de tecnologia energética podem adquirir subcomponentes de centenas de fabricantes diferentes para um único equipamento; essa tecnologia pode, por sua vez, ser adquirida por outro fornecedor e integrada a um sistema adicional antes de chegar ao usuário final." Para que os usuários finais tenham confiança em seus sistemas, eles precisam confiar que toda a cadeia de suprimentos segue os mesmos princípios de segurança.[34]

masterplan-2024/
[32] https://www.rajahtannasia.com/viewpoints/singapore-launches-updated-national-operational-technology-cybersecurity-masterplan/
[33] https://www.energy.gov/ceser/supply-chain-cybersecurity-principles
[34] https://www.energy.gov/ceser/supply-chain-cybersecurity-principles

NIST SP 800-82 Rev. 3: Guia para a Segurança da Tecnologia Operacional (OT)

Em 2023, o NIST publicou o SP 800-82 Rev. 3: Guia para a Segurança em Tecnologia Operacional (OT).[35] O documento fornece orientações abrangentes sobre como garantir a segurança OT, "ao mesmo tempo em que atende aos requisitos únicos de desempenho, confiabilidade e segurança."[36] Além de uma explicação sobre OT, segurança OT e como OT se encaixa em diferentes ambientes de sistema, o documento também oferece uma visão geral de "OT" e topologias típicas de sistema, identifica ameaças e vulnerabilidades comuns a esses sistemas e lista as contramedidas de segurança recomendadas para mitigar os riscos associados.

O guia apresenta uma abordagem baseada em risco para proteger ambientes OT, incluindo boas práticas como estratégias de defesa aprofundada, avaliações regulares de riscos e vulnerabilidades, e processos robustos de resposta e recuperação a incidentes. Também vincula as práticas de cibersegurança em TO com estruturas mais amplas, como o NIST Cybersecurity Framework e os controles de segurança NIST SP 800-53, que permitem que organizações incluam a segurança OT em programas de gestão de riscos em toda a empresa.[37]

Recomendações

Uma regulamentação eficaz da cibersegurança deve diferenciar as obrigações entre operadores de infraestrutura crítica e provedores de soluções tecnológicas por meio de um quadro de responsabilidade compartilhada. Operadores de infraestrutura crítica — entidades que operam diretamente sistemas essenciais como redes de energia, sistemas de água ou redes de telecomunicações — têm a responsabilidade primária de proteger seus ambientes operacionais, incluindo avaliações de risco, resposta a incidentes e controles de segurança adequados às suas operações. Provedores de soluções tecnológicas, como provedores de serviços em nuvem, redes de entrega de conteúdo e serviços de armazenamento de dados, mantêm a segurança de suas plataformas e serviços por meio de certificações do setor e obrigações contratuais, enquanto os operadores mantêm a responsabilidade pela segurança no uso desses serviços, incluindo decisões de configuração e controle de acesso.

As regulamentações devem reconhecer explicitamente o Princípio da Responsabilidade Compartilhada e distribuir obrigações de prevenção, proteção, resposta e recuperação entre os atores públicos e privados do sistema digital, de acordo com seu papel específico, nível de exposição e capacidade operacional. Essa abordagem baseada em riscos e neutra em relação à tecnologia garante que a responsabilidade

[35] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf
[36] https://csrc.nist.gov/pubs/sp/800/82/r3/final
[37] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf

esteja alinhada com o controle operacional real, permite que operadores de infraestrutura escolham provedores com base em capacidades de segurança em vez de classificação regulatória, e promove um ambiente regulatório que aprimora a segurança ao mesmo tempo em que possibilita transformação digital e acesso a capacidades avançadas de segurança em nuvem.

Aprendendo com a pesquisa e as melhores práticas, o artigo apresenta as seguintes recomendações.

Plano para Segurança da Terapia Ocupacional

Organizações responsáveis pela infraestrutura crítica devem estabelecer responsabilidade clara pela segurança operacional da tecnologia (OT). Seja a segurança de TO gerenciada dentro de uma equipe de cibersegurança de TI existente ou por meio de uma função dedicada de segurança de TO, deve haver pessoal especificamente encarregado de proteger sistemas de controle industrial e ativos relacionados. Sem uma propriedade definida, as iniciativas de cibersegurança em OT frequentemente perdem prioridade e são negligenciadas, deixando sistemas críticos expostos a riscos evitáveis. Estabelecer liderança, responsabilidade e uma estratégia formal garante que ambientes de TO recebam atenção, recursos e gestão de riscos consistentes.

Mapeamento da Convergência de TI/OT

À medida que os sistemas de TI e OT se tornam cada vez mais interconectados, as organizações precisam mapear claramente como esses ambientes interagem. Historicamente, os sistemas industriais eram isolados, mas a modernização e a transformação digital introduziram novos pontos de conectividade e potencial vulnerabilidade. Uma visão clara de onde as redes de TI e OT interagem permite que as organizações identifiquem riscos, esclareçam responsabilidades de governança e implementem controles de segurança apropriados. A convergência do mapeamento também permite uma melhor coordenação entre as equipes de TI e OT, garantindo que políticas, monitoramento e processos de resposta a incidentes levem em conta as realidades dos ambientes integrados.

Proteja a Cadeia de Suprimentos

A cibersegurança para infraestrutura crítica deve se estender além dos operadores individuais para incluir toda a cadeia de suprimentos. Governos e operadores de infraestrutura deveriam exigir padrões básicos de OT e cibersegurança de TI de fornecedores, fabricantes, integradores e prestadores de serviços. Como diferentes atores interpretam papéis diferentes, os requisitos devem ser adaptados de acordo. Por exemplo, os fabricantes podem precisar atender a padrões de desenvolvimento e patch seguros, enquanto proprietários e operadores devem manter práticas seguras de configuração e monitoramento. Estabelecer expectativas consistentes

na cadeia de suprimentos ajuda a reduzir riscos sistêmicos e previne vulnerabilidades introduzidas por produtos ou serviços de terceiros.

Secure-by-Design / Secure-by-Default

A adoção dos princípios de secure-by-design e secure-by-default ajuda a mitigar riscos de cibersegurança antes da implantação dos sistemas. Em vez de depender apenas de medidas defensivas após a descoberta de vulnerabilidades, essas abordagens enfatizam a construção de segurança em tecnologias e processos desde o início. Isso inclui o design de sistemas com autenticação forte, serviços expostos mínimos, configurações seguras e mecanismos robustos de atualização habilitados por padrão. Incentivar fabricantes e operadores a priorizarem a segurança durante o desenvolvimento e a implantação reduz a probabilidade de vulnerabilidades exploráveis e fortalece a resiliência de longo prazo dos sistemas críticos de infraestrutura.

Fortaleça a Resposta Coordenada a Incidentes e a Recuperação

A proteção eficaz da infraestrutura crítica exige capacidades robustas e coordenadas de resposta a incidentes e recuperação, tanto no setor público quanto no privado. Governos e operadores devem estabelecer estruturas claras para o compartilhamento de informações, permitindo a troca oportuna de inteligência sobre ameaças, vulnerabilidades e dados de incidentes, respeitando a confidencialidade e as restrições legais. Fortalecer canais de comunicação confiáveis entre operadores de infraestrutura, reguladores e autoridades de cibersegurança pode melhorar significativamente a consciência situacional e a eficácia da resposta.

Testes regulares por meio de exercícios conjuntos, como simulações de incidentes cibernéticos que afetam ambientes de TI e OT, ajudam a garantir que papéis, responsabilidades e procedimentos de resposta sejam bem compreendidos e operacionais. Além disso, o planejamento da recuperação deve ser priorizado junto com os esforços de resposta, incluindo o desenvolvimento de estratégias de continuidade de negócios e restauração de sistemas adaptadas aos contextos críticos de infraestrutura. Dada a natureza interconectada dos sistemas digitais, mecanismos de cooperação transfronteiriça também são essenciais na América Latina para enfrentar ameaças transnacionais, coordenar respostas e apoiar a rápida recuperação de incidentes de grande escala.

Invista em uma força de trabalho mais forte

A cibersegurança para infraestrutura crítica na América Latina exige investimento contínuo no desenvolvimento da força de trabalho, especialmente para profissionais que atuam na interseção entre TI e ambientes de TO. Muitos países da região carecem de profissionais qualificados em cibersegurança com expertise especializada em sistemas de controle industrial, o que deixa lacunas na proteção de serviços essenciais. Governos e partes interessadas da indústria devem priorizar o desenvolvimento de programas direcionados de educação e treinamento focados na segurança da OT, incluindo parcerias com universidades, institutos

técnicos e órgãos internacionais de certificação.

Expandir o acesso a certificações padronizadas e treinamentos práticos pode ajudar a construir um pipeline de profissionais qualificados capazes de enfrentar ameaças em constante evolução. Ao cultivar uma força de trabalho de cibersegurança altamente qualificada e estável, os países latino-americanos podem ampliar sua capacidade de gerenciar riscos, responder a incidentes e manter resiliência de longo prazo em setores de infraestrutura crítica.

Conclusão

À medida que a América Latina continua modernizando sua infraestrutura e expandindo a conectividade digital, a segurança da infraestrutura crítica deve permanecer uma prioridade central para governos, operadores e parceiros da indústria. A convergência dos ambientes de TI e OT, a crescente dependência de serviços em nuvem e inteligência artificial, e a complexidade crescente das cadeias globais de suprimentos remodelaram fundamentalmente o cenário de risco para setores críticos. Ao mesmo tempo, o aumento da atividade cibernética patrocinada pelo Estado — especialmente da China e da Rússia — introduziu um ambiente de ameaças mais estratégico e persistente, no qual adversários buscam não apenas explorar vulnerabilidades, mas também se pré-posicionar dentro de sistemas críticos para possíveis interrupções durante crises geopolíticas. Os resultados da pesquisa apresentados neste artigo destacam tanto o progresso encorajador quanto as lacunas persistentes, especialmente nas áreas de planejamento de segurança específico para OT, visibilidade da cadeia de suprimentos e preparação para ameaças emergentes.

As experiências de outras jurisdições demonstram que a proteção eficaz da infraestrutura crítica requer estratégias coordenadas que combinem liderança política, estruturas regulatórias, padrões do setor e colaboração público-privada. Estratégias nacionais de cibersegurança que abordam explicitamente a tecnologia operacional, estruturas dedicadas à segurança de OT, princípios de segurança da cadeia de suprimentos e regulamentações regionais harmonizadas podem contribuir para a construção de sistemas mais resilientes. Ao mesmo tempo, as organizações responsáveis pela infraestrutura crítica devem fortalecer a governança interna, mapear as interseções entre ambientes de TI e OT, e adotar práticas de segurança desde o projeto que incorporem a segurança ao longo de todo o ciclo de vida da tecnologia.

Em última análise, proteger infraestrutura crítica não é apenas um desafio de cibersegurança, mas sim um requisito estratégico para a estabilidade econômica, segurança pública e resiliência nacional. A crescente prevalência de campanhas como Volt Typhoon e Salt Typhoon ilustra ainda mais que infraestrutura crítica é agora um ponto focal de competição estratégica de longo prazo, exigindo que governos e operadores se preparem tanto para ameaças imediatas quanto para riscos latentes e pré-posicionados dentro de suas redes. Ao aprender com as melhores práticas globais e investir em governança mais forte, desenvolvimento da força de trabalho e cooperação intersetorial, os países latino-americanos podem reduzir o risco sistêmico e construir sistemas de infraestrutura mais seguros e confiáveis, capazes de apoiar o crescimento de longo prazo e a estabilidade regional.


DIGI
AMERICAS