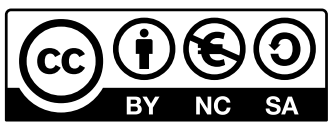
COMPARTILHAMENTO DE INFORMAÇÕES NA LATAM:

COMPREENDENDO O PAPEL DOS ISACS NA REGIÃO

DIGI AMERICAS



Para mais informações, entre em contato através do e-mail: admin@digiamericas.org

Digi Americas Alliance

Alain Karioty
Alexis Steffaro
Andrea Escobedo
Andy Kotz
Belisario Contreras
Brett DeWitt
Carlos Torales
Christian Torres
Cory Bullock
Fernando Quintero
Gene Yoo
Ghassan Dreibi
Hernan Armbruster
Jordana Siegel
José Juan Haro
Mario de la Cruz Sarabia
Mauricio Benavides
Mauricio Nanne
Norberto (Bert) Milan
Patrick Ford
Rafael Alvarez
Ricardo Villadiego
Ryan Goss

Editores

Belisario Contreras
Alexis Steffaro
Pallavi Bhargava

DIGI AMERICAS ALLIANCE MEMBERS

aws Apple CHECK POINT CISCO CLOUDFLARE CROWDSTRIKE fluid attacks we hack your software Google
kriptos LUMU METABASE Q netskope paloalto NETWORKS Resecurity
Santander Schneider Electric Telefónica tenable Trellix TREND MICRO

Resumo

A rápida transformação digital na América Latina e Caribe (LATAM) aumentou significativamente a vulnerabilidade da região a ataques cibernéticos. Além disso, a abordagem fragmentada no compartilhamento de informações sobre segurança cibernética tem limitado a capacidade de resposta a incidentes. Este documento analisa o papel dos Centros de Compartilhamento e Análise de Informações (Information Sharing and Analysis Centers - ISACs) como uma solução para fortalecer a resiliência da região. O documento apresenta uma visão geral das estruturas dos ISACs, seus modelos de governança e os benefícios que oferecem aos membros, destacando seu potencial para enfrentar os desafios únicos de cibersegurança na LATAM. Ao analisar as iniciativas de compartilhamento de informações já existentes na região, ele aponta lacunas importantes, como a falta de integração entre os esforços dos setores público e privado. A análise reforça a necessidade de ISACs escaláveis e formalizados, adaptados às realidades operacionais e culturais da LATAM. Embora este documento não proponha uma estrutura específica para os ISACs, ele ressalta a importância de criar modelos que se ajustem ao contexto único da região. Além de estabelecer ISACs formalizados, é recomendável aproveitar as iniciativas de compartilhamento de informações já existentes e conectá-las a redes globais de ISACs sempre que for adequado. Essas estratégias têm como objetivo fomentar o engajamento de diversos atores, reduzir as disparidades na maturidade em cibersegurança e capacitar os stakeholders regionais a adotar mecanismos colaborativos que fortaleçam a resiliência e enfrentem as ameaças específicas da LATAM.

Sumário

Introdução

A região da América Latina e Caribe (LATAM) tem se tornado cada vez mais dependente de infraestrutura digital. Após a pandemia de COVID-19, muitos serviços essenciais, como bancos e saúde, passaram a ser digitalizados, o que os tornou mais vulneráveis a ataques cibernéticos. Na Colômbia, por exemplo, 72% de todas as transações financeiras são realizadas por canais digitais.[1] Com essa crescente dependência da tecnologia, é fundamental a implementação de estratégias digitais inovadoras e protocolos de segurança. Diversos atores privados na região têm destacado essa necessidade e pedido mudanças. O Centro México Digital revelou que "47% das empresas latino-americanas reconhecem a importância de uma estratégia digital e o papel essencial da tecnologia da informação na continuidade dos negócios". Até 2023, 72% das empresas na região já haviam iniciado o processo de digitalização de suas operações. Além disso, México e Brasil figuram entre os 10 países com o maior número de usuários de internet no mundo.[2] No entanto, em 2021, apenas três países da América Latina haviam implementado uma estratégia digital nacional. Embora esse número tenha crescido desde então, ainda há uma grande disparidade no progresso entre os setores público e privado.[3]

A crescente dependência digital e o mercado de cibersegurança em expansão tornam a LATAM altamente vulnerável a ataques cibernéticos. Até 2025, a região pode enfrentar uma média de mais de 18,5 milhões de ataques por ano, com custos anuais superiores a US$ 90 milhões.[4] Os ataques de ransomware têm sido os mais frequentes e prejudiciais, com países como Colômbia, Brasil, Costa Rica, Chile e Panamá enfrentando grandes e altamente disruptivos ataques nos últimos anos.[5] O ransomware é um tipo de malware que impede os usuários de acessar seus dispositivos ou dados, geralmente criptografando os arquivos. Os criminosos exigem um resgate em troca da chave para descriptografá-los. No Panamá, por exemplo, os ataques cibernéticos aumentaram 421% nos últimos dois anos.[6] Em 2023, o mercado de cibersegurança na América Latina foi avaliado em US$ 8,34 bilhões, com previsão de crescimento anual de cerca de 6,95% entre 2023 e 2028, superando os US$ 11 bilhões até 2028.[7]

---

[1] La Republica, Las transacciones digitales ya representan 72% dentro de las operaciones de los bancos, June 21, 2021. Disponível em: https://www.larepublica.co/finanzas/las-transacciones-digitales-ya-representan-72-dentro-de-las-operaciones-de-los-bancos-3187260#:~:text=Es%20decir%20m%C3%A1s%20de%2072,y%20con%20d-at%C3%A1fonos%20692%20millones.
[2] BN Americas, Companies Embracing Change in Latin Americas Digital Transformation, January 24, 2024. Disponível em: https://www.bnamericas.com/en/news/companies-embracing-change-in-latin-americas-digital-transformation.
[3] Financial Services ISAC, Emerging Trends to Cyber Risks: a Latin American Perspective. Disponível em: https://www.fsisac.com/insights/emerging-trends-to-cyber-risks-latin-american-perspective. Acesso em: 26 jul. 2024.
[4] Digi Americas, Cyber Readiness in Latin American Public Sectors, 2024. Disponível em: https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf.
[5] Ibid.
[6] Ibid.
[7] Statista, Value of the Cybersecurity Market in Latin America in 2023 and 2028, Jan. 2, 2024. Disponível em: https://www.statista.com/statistics/1180184/value-cybersecurity-market-latin-america/.

Há grandes lacunas de maturidade cibernética entre os países da LATAM, o que resulta em uma resiliência desigual e respostas inconsistentes a incidentes na região. A "lacuna de maturidade cibernética" refere-se à diferença entre as capacidades atuais de cibersegurança de um país ou organização e o nível necessário de maturidade, geralmente medido por meio de um framework de segurança reconhecido. Os países da LATAM estão em estágios diferentes no desenvolvimento de suas políticas de cibersegurança, o que leva a variações significativas nas táticas de identificação e nas práticas de resposta a incidentes.

A região precisa de um mecanismo coeso de compartilhamento de informações para fortalecer sua resiliência.

Ao compartilhar rapidamente dados críticos sobre ataques cibernéticos e vulnerabilidades generalizadas, é possível reduzir consideravelmente a gravidade e a extensão dos incidentes cibernéticos.[8] Com a LATAM se tornando cada vez mais alvo de atores maliciosos, a região precisa de um fórum coeso que reúna todos os stakeholders relevantes, tanto do setor público quanto do privado, para compartilhar informações sobre ameaças e melhores práticas. Os Centros de Compartilhamento e Análise de Informações (ISACs) são comuns nos EUA e na Europa, funcionando como um ponto central para reunir e disseminar dados sobre ameaças cibernéticas a infraestruturas críticas de um setor específico.[9] Tanto os governos quanto os participantes do setor privado na LATAM reconheceram a necessidade de uma iniciativa semelhante na região, mas sabem que isso exigirá uma abordagem adaptada à realidade local.

Atualmente, os esforços de compartilhamento de informações na LATAM são fragmentados, com os setores público e privado operando de forma isolada, em vez de colaborarem entre si. Essa falta de integração limita as oportunidades para uma troca eficaz de informações valiosas. Os desafios são ainda maiores devido a características regionais, como o receio de parecer vulnerável ao compartilhar dados sobre ameaças, a preferência cultural por trocas informais e a necessidade de lidar com ameaças específicas da região, como o malware Mekotio, um trojan bancário que afeta particularmente a LATAM.[10] Este documento tem como objetivo explorar os fatores essenciais para a criação de ISACs na LATAM. Em vez de defender um modelo único, ele destaca a importância de iniciativas formalizadas e escaláveis que complementem e fortaleçam as

[8] Cybersecurity and Infrastructure Security Agency (CISA), Information Sharing. Disponível em: https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing#:~:text=By%20rapidly%20sharing%20critical%20information,events%20can%20be%20greatly%20decreased. Acesso em: 27 set. 2024.
[9] National Council of ISACs, About ISACs. Disponível em: https://www.nationalisacs.org/about-isacs. Acesso em: 19 jul. 2024.
[10] Trend Micro, Mekotio Banking Trojan Threatens Financial Systems in Latin America, July 4, 2024. Disponível em: https://www.trendmicro.com/en_us/research/24/g/mekotio-banking-trojan.html.

abordagens informais já em prática. Seja em nível setorial ou nacional, os ISACs na LATAM devem estar alinhados com as dinâmicas culturais e operacionais da região, aproveitando as práticas atuais de compartilhamento de informações e se conectando a redes globais de ISACs quando necessário.

O objetivo deste documento é fornecer aos stakeholders as informações necessárias para decidir sobre a estrutura de ISAC mais adequada às suas necessidades, destacando os benefícios, desafios e as bases existentes para o compartilhamento de informações na LATAM. Uma colaboração aprimorada na região pode ajudar a reduzir as lacunas de maturidade, aumentar a resiliência, fortalecer a confiança e enfrentar as ameaças de forma alinhada às características únicas da região.
O restante do documento começa com uma introdução aos ISACs, abordando seu histórico, propósito, principais benefícios e desafios, diferentes modelos estruturais, papéis e responsabilidades, opções de governança e financiamento, e principais competências. Em seguida, avalia criticamente a necessidade de ISACs formalizados na LATAM, utilizando exemplos específicos da região para mostrar como esses modelos se alinham com políticas emergentes e o desejo de maior colaboração entre múltiplos stakeholders. O documento prossegue com uma visão geral das iniciativas ad hoc de compartilhamento de informações existentes na LATAM, destacando seus principais sucessos e desafios. Por fim, a conclusão recomenda que, independentemente da estrutura adotada, a LATAM se beneficiaria de mecanismos formalizados de compartilhamento de informações, que aproveitem os esforços já em andamento e vão além do simples compartilhamento de dados, incorporando também iniciativas de educação e desenvolvimento da força de trabalho. Com essas mudanças, seria possível avançar no fechamento das amplas lacunas de maturidade cibernética que existem na região.


50%
90%
100%

Componentes de um ISAC

Um ISAC, conforme definido nos EUA, é uma organização sem fins lucrativos, baseada em associação, que serve como um ponto central para coletar, analisar e disseminar informações sobre ameaças relevantes para seus membros, promovendo o compartilhamento bidirecional de dados entre os setores privado e público. Os ISACs podem ter diferentes estruturas, variando desde modelos compostos exclusivamente por representantes do setor privado até aqueles que incluem participantes do governo e da sociedade civil. Embora muitos ISACs existentes operem apenas no setor privado, este documento defende uma abordagem multissetorial, baseada nas práticas atuais, para promover maior inclusão e colaboração. Os ISACs criam um ecossistema de confiança entre seus membros, permitindo que os responsáveis por infraestruturas críticas protejam melhor a si mesmos e seus clientes contra ameaças cibernéticas e físicas. Eles oferecem alertas sobre ameaças e relatórios de incidentes 24 horas por dia, além de promoverem reuniões anuais, troca de conhecimento técnico, workshops e webinars. Embora sejam uma forma de parceria público-privada (PPP), os ISACs são considerados mais formais do que as PPPs tradicionais, pois seus membros seguem um framework bem definido para o compartilhamento de informações e análises. Enquanto a maioria dos ISACs nos EUA e na União Europeia adota uma abordagem focada em setores específicos, a próxima seção explora os diferentes modelos estruturais para a criação de um ISAC, que serão importantes para a comunidade da LATAM considerar ao iniciar a formalização do compartilhamento de informações na região.

HISTÓRIA E ADOÇÃO INTERNACIONAL

O conceito de ISACs foi introduzido pela Presidential Decision Directive-63 (PDD-63) dos EUA, assinada em 22 de maio de 1998. A partir dessa diretiva, o governo federal solicitou que cada setor de infraestrutura crítica criasse organizações específicas para compartilhar informações sobre ameaças e vulnerabilidades.[11] Alguns dos ISACs mais conhecidos nos EUA incluem o Financial Services ISAC (FS-ISAC), o Health ISAC (H-ISAC), o Information Technology ISAC (IT-ISAC) e o Multi-State ISAC (MS-ISAC), entre outros.[12] Esses ISACs setoriais colaboram entre si por meio do National Council of ISACs (NCI), uma entidade coordenadora que visa maximizar o intercâmbio de informações entre as infraestruturas críticas do setor privado e o governo. [13] O NCI oferece um fórum para o compartilhamento de informações sobre ameaças e estratégias de mitigação entre os ISACs, bem como com parceiros governamentais e do setor privado, especialmente durante incidentes que exigem uma resposta coordenada entre

[11] National Council of ISACs, About ISACs.
[12] National Council of ISACs, Member ISACs. Disponível em: https://www.nationalisacs.org/members. Acesso em: 19 jul. 2024.
[13] Ibid.

setores. Com reuniões regulares, o NCI coordena as operações dos centros ISACs e organiza exercícios e atividades conforme necessário.[14] A divisão dos ISACs por setores de infraestrutura crítica permite que a plataforma mantenha uma visão situacional específica para cada setor, considerando as particularidades de cada um. Embora a maioria dos ISACs nos EUA tenha foco em membros locais, ISACs mais estabelecidos, como o FS-ISAC, contam com empresas associadas internacionalmente, incluindo na LATAM.[15] Por exemplo, grandes multinacionais costumam ser membros de ISACs nos EUA e podem participar de mais de um, conforme seus interesses e áreas de atuação.

À medida que os ISACs cresceram em número e maturidade nos EUA, eles também foram adotados na União Europeia (UE) de maneiras variadas. Na UE, os ISACs podem ser formais ou informais, focados em países, setores específicos ou de alcance internacional. Os primeiros ISACs europeus se concentraram nos setores financeiro e de energia. A abordagem da UE para os ISACs é única, pois geralmente envolve o apoio governamental, especialmente para funções facilitadoras, além da oferta de expertise e conhecimento como parceiro do ISAC.[16] Além disso, a legislação europeia apoia a criação de ISACs. A Diretiva NIS 2, por exemplo, categoriza os operadores de serviços essenciais por setores e os responsabiliza pela implementação de requisitos relacionados à notificação de incidentes[17]. A criação de ISACs setoriais em nível nacional pode facilitar a implementação dessas normas, servindo como ponto de interação entre os stakeholders do setor público e privado.[18] À medida que a LATAM avança em sua legislação de cibersegurança, os governos da região devem considerar a inclusão de disposições que incentivem a criação de mecanismos de compartilhamento de informações, à semelhança do que acontece na UE.

No entanto, é importante destacar que essa abordagem gerou controvérsias, já que muitos ISACs baseados nos EUA têm uma presença significativa na UE, o que resultou em confusão e na necessidade de alinhar papéis e responsabilidades sobrepostos. A LATAM deve considerar essa complexidade ao desenvolver sua legislação e iniciativas de cibersegurança. Governos e stakeholders na LATAM podem se beneficiar ao identificar proativamente oportunidades de parceria com comunidades globais de compartilhamento de informações já existentes, a fim de reduzir a fragmentação, aproveitar o conhecimento consolidado e lidar com as limitações orçamentárias. Essas parcerias podem diminuir a necessidade de criar novos sistemas do zero, garantindo soluções mais econômicas e baseadas em modelos comprovados. Ao levar esses fatores em conta, a LATAM pode criar mecanismos de compartilhamento de informações que equilibrem a relevância regional com as oportunidades de cooperação internacional, aprendendo tanto com os sucessos quanto com os desafios da experiência europeia.

---

[14] National Council of ISACs, About NCI. Disponível em: https://www.nationalisacs.org/about-nci. Acesso em: 9 out. 2024.
[15] Financial Services ISAC, Emerging Trends to Cyber Risks: A Latin American Perspective.
[16] ENISA, ISACs Cooperative Models.
[17] NIS 2 Directive. Disponível em: https://www.nis-2-directive.com. Acesso em: 22 out. 2024.
[18] Ibid.

PRINCIPAIS BENEFÍCIOS

Postura de Segurança Aprimorada e Defesa Coletiva

O principal benefício de um ISAC é proporcionar defesa coletiva. Se uma organização está sendo alvo de um ataque cibernético, é provável que outras organizações na região, ou até mesmo globalmente, também estejam. Ao compartilhar informações, melhores práticas ou medidas de remediação de ataques anteriores, os membros do ISAC podem ajustar suas defesas conforme necessário. Isso também incentiva ações proativas contra vulnerabilidades compartilhadas dentro do ISAC, evitando que os membros aguardem a ocorrência de um desastre para agir.[19]

Especialização em Cibersegurança Baseada na Comunidade

Entidades menores frequentemente não têm os recursos necessários para monitorar ameaças de forma contínua, avaliar impactos e desenvolver planos robustos de mitigação. Obter financiamento, recursos e pessoal para iniciativas de cibersegurança é um desafio, por isso, participar de um ISAC permite que as organizações se beneficiem da expertise compartilhada com seus parceiros. Os membros do ISAC têm acesso a webinars, workshops educativos e canais de comunicação seguros, que facilitam a troca rápida e confiável de informações. Se uma organização-membro tiver dúvidas específicas sobre seu setor, pode contar com a rede de colegas do ISAC para respostas, em vez de precisar realizar pesquisas demoradas e custosas. Além disso, os ISACs têm um histórico de responder e compartilhar informações acionáveis e relevantes de forma mais ágil do que os parceiros governamentais.[20]

Maior Confiança e Resiliência na Comunidade

Os ISACs promovem maior confiança e um forte senso de comunidade entre seus membros, criando um ambiente onde a colaboração e o apoio mútuo são prioritários. Essa confiança é fundamental para lidar com as ameaças cibernéticas em constante evolução, pois estimula o compartilhamento proativo e oportuno de informações valiosas. Além do compartilhamento de inteligência, os ISACs ajudam seus membros a desenvolverem, coletivamente, uma postura de segurança mais robusta, reunindo recursos e expertise que muitas vezes são inacessíveis para organizações isoladas. Ao aproveitar essa rede de apoio, os ISACs aumentam a segurança da informação e a resiliência contra ameaças cibernéticas, reduzindo os custos adicionais para seus membros. [21] Além disso, os ISACs desempenham um papel importante na promoção

---

[19] Health Sector Coordinating Council Cybersecurity Working Group, Health Industry Cybersecurity - Information Sharing Best Practices, Aug. 2023. Disponível em: https://healthsectorcouncil.org/wp-content/uploads/2023/08/HIC-ISBP-2023.pdf.
[20] National Council of ISACs, About ISACs.
[21] Health Sector Coordinating Council Cybersecurity Working Group, Health Industry Cybersecurity - Information Sharing Best Practices, Aug. 2023. Disponível em: https://healthsectorcouncil.org/wp-content/uploads/2023/08/HIC-ISBP-2023.pdf.

da alfabetização digital e no desenvolvimento de habilidades de comunicação, colaboração e resolução de problemas entre seus membros – princípios que se alinham com a estrutura de alfabetização digital da UNESCO. [22] Esse senso de comunidade, somado aos benefícios práticos, torna os ISACs essenciais em um cenário digital cada vez mais interconectado.

Inovação em Cibersegurança Aprimorada

Ao aumentar a conscientização sobre ameaças em todo o setor por meio do compartilhamento de informações, as organizações recebem alertas antecipados e podem adotar medidas proativas para mitigar possíveis ataques. À medida que os ataques se tornam mais sofisticados, especialmente com a integração da IA generativa, que potencializa as capacidades dos invasores, as equipes de segurança precisam garantir que suas organizações se adaptem aos novos desafios, padrões e melhores práticas do setor para manter suas operações seguras. O envolvimento com parceiros setoriais por meio dos ISACs permitirá que as organizações acompanhem essa evolução de forma eficaz.

Benefícios para o Governo

A colaboração estreita com o setor privado permite que os órgãos públicos compreendam melhor os desafios específicos de cada área, o que é essencial para a formulação de legislações e estratégias de cibersegurança. Ao participar dos ISACs, o governo pode obter informações valiosas sobre a postura de segurança de setores-chave, por meio do compartilhamento de dados sobre ameaças, incidentes e vulnerabilidades. Essa participação, quando conduzida com respeito aos diferentes níveis de tolerância ao compartilhamento de informações com o setor público, pode ajudar a melhorar a compreensão do cenário cibernético em constante evolução e fortalecer a capacidade do governo de apoiar setores críticos. Além disso, essa colaboração aprimora a comunicação e a coordenação, garantindo que as políticas e estratégias sejam baseadas em informações concretas e alinhadas às necessidades reais dos setores que se busca proteger.

[22] The World Bank, Digital Economy for Latin America and the Caribbean Country Diagnostic: Jamaica, pg. 118, April 2024. Disponível em: https://thedocs.worldbank.org/en/doc/61714f214ed04bcd6e9623ad0e215897-0400012021/related/IDU1c6883bf81f279148581a6dd184a5f721a2ea.pdf.

DESAFIOS DOS ISACs

Embora participar de um ISAC ofereça diversos benefícios para os membros e para o ecossistema de cibersegurança como um todo, existem desafios que podem dificultar o sucesso do compartilhamento de informações.

Falta de Recursos/Financiamento

O principal desafio para os membros públicos e privados dos ISACs é a escassez de recursos humanos e financeiros para dedicar ao compartilhamento e análise de informações. Esse é um problema comum no setor de cibersegurança, mas se torna ainda mais complicado quando se trata da análise de dados. Organizações com poucos funcionários não conseguem participar ativamente do ISAC, e os governos podem não ter a capacidade de preencher funções essenciais, como secretariado ou facilitadores. A falta de financiamento e de pessoal dedicado também pode ser um obstáculo para pequenas e médias empresas. Empresas maiores, com mais recursos, têm mais condições de arcar com a adesão, o que pode fazer com que elas dominem os ISACs, deixando as empresas menores – que mais precisariam dessa colaboração – de fora. Além disso, a diversidade de níveis de maturidade e conhecimento em cibersegurança entre os membros pode dificultar a compreensão das informações compartilhadas. Por isso, é fundamental que os ISACs adaptem os recursos compartilhados para que sejam acessíveis a todos, independentemente do porte ou nível de maturidade das organizações. Muitos ISACs investem as taxas de adesão em programas de treinamento e capacitação, oferecendo aos membros um nível maior de especialização técnica.[23] No entanto, a falta de financiamento pode afetar a qualidade da análise fornecida aos participantes.

Nível Mínimo de Expertise/Participação

Devido aos diferentes níveis de maturidade, os participantes de um ISAC precisam ter um conjunto mínimo de habilidades técnicas e organizacionais para se envolver ativamente nas atividades de compartilhamento de informações e nos exercícios. Para que a colaboração seja bem-sucedida, é importante estruturar o modelo com incentivos que promovam o compartilhamento ativo de informações, garantindo que todos os membros participem. Além disso, é fundamental envolver não apenas a equipe técnica, mas também executivos de alto nível nas atividades de troca de informações e nos treinamentos. Isso ajuda a demonstrar o valor do ISAC para a liderança da organização, facilitando a alocação de recursos financeiros necessários para essas iniciativas.

---

[23] Ibid.

Construção de Confiança/Diferenças Culturais

Questões relacionadas à privacidade e confidencialidade são sempre uma preocupação para os membros potenciais dos ISACs. No entanto, os ISACs existentes implementam medidas rigorosas de proteção de dados, como controles de acesso restritos, técnicas de anonimização e canais de comunicação seguros.[24] Além disso, esses centros consultam especialistas jurídicos para garantir conformidade com as regulamentações de privacidade e manter-se atualizados sobre mudanças nas leis.[25] O objetivo é equilibrar o compartilhamento aberto e produtivo de informações com a proteção da privacidade. Outros desafios podem envolver barreiras linguísticas, diferenças culturais ou variação nos níveis de especialização. Para superar essas questões, os ISACs frequentemente oferecem serviços de tradução e padronizam os formatos e protocolos de compartilhamento de informações, tornando o processo mais acessível entre os setores.[26] Dessa forma, o compartilhamento de informações em um ISAC se torna uma das formas mais seguras e confiáveis de comunicação intersetorial, com um forte compromisso com a privacidade e a segurança. Embora a ideia de compartilhar informações para prevenir ameaças possa parecer contraintuitiva, os ISACs operam de maneira ética e transparente, onde todos os membros são tratados igualmente.

Papéis e Responsabilidades Claros

A flexibilidade dos diferentes modelos de estrutura, governança e atribuição de papéis e responsabilidades dos ISACs pode ser um desafio para organizações que buscam estabelecer ou participar dessas iniciativas. Embora essa flexibilidade permita adaptar o modelo às necessidades de cada setor e contexto regional, ela também pode gerar inconsistências no compartilhamento e gerenciamento de informações. Diferentes estruturas de governança podem causar confusão nos processos de tomada de decisão e na definição de responsabilidades, tornando difícil para os membros entenderem claramente seus papéis. Além disso, os variados níveis de comprometimento e de alocação de recursos entre os membros podem levar a uma participação desigual, o que pode prejudicar a eficácia do ISAC. A falta de padronização também pode dificultar a colaboração e reduzir a confiança necessária para um compartilhamento eficaz de informações. Esses desafios são ainda mais evidentes em regiões como a América Latina, onde há grandes disparidades na maturidade organizacional em termos de compreensão e preparo para a cibersegurança. Contudo, esses obstáculos podem ser minimizados com uma abordagem mista, que combine modelos baseados em países e foque em setores-chave com maior maturidade, como o setor financeiro. Esse alinhamento estratégico

[24] Blue Goat Cyber, The Impact of Information Sharing Analysis Centers on Cybersecurity. Disponível em: https://bluegoatcyber.com/blog/the-impact-of-information-sharing-and-analysis-centers-on-cybersecurity. Acesso em: 26 jul. 2024.
[25] Ibid.
[26] Ibid.

permite soluções mais personalizadas, favorecendo a colaboração, aumentando a confiança e, em última instância, fortalecendo a postura de cibersegurança da região.

MODELOS ESTRUTURAIS

Existem diferentes maneiras de organizar um ISAC, mas dois modelos principais se destacam:

- Modelo focado no país
- Modelo por setor específico

Modelo Focado no País

Esse modelo de cooperação concentra-se em um único país, reunindo especialistas e equipes de resposta a incidentes de segurança cibernética (CSIRTs) em uma única iniciativa. O modelo focado no país pode resultar em arranjos informais, onde a comunidade de CSIRTs gerencia a cooperação, ou em formas mais formalizadas, com o governo do país desempenhando um papel coordenador. ISACs facilitados pelo governo são mais comuns em países menores, onde é mais viável para o setor público gerenciar um ISAC devido ao número reduzido de partes interessadas. Abaixo, apresentamos alguns exemplos de ISACs focados em países:

» **CERT.LU** – Uma iniciativa nacional que reúne todas as equipes de resposta a emergências cibernéticas (CERTs) em Luxemburgo, com o objetivo de facilitar a troca de informações entre os CSIRTs do país.[27] Esse ISAC é gerido pela própria comunidade CERT.[28]

» **Finlândia** – Diversos ISACs são coordenados pelo Centro Nacional de Cibersegurança (NCSC-FI). O NCSC-FI coleta e analisa informações sobre ameaças cibernéticas provenientes de diversas fontes, como ISACs e sistemas de alerta precoce, e compartilha esses dados com seus membros por meio de diversos canais, incluindo os ISACs.[29]

Modelo por Setor Específico

Este modelo foca na infraestrutura crítica de um setor específico, com o objetivo de compartilhar informações e análises entre especialistas ativos nesse setor. Normalmente, a liderança vem de partes interessadas do setor privado, com pouca ou nenhuma contribuição governamental, especialmente nos EUA, onde o financiamento público para ISACs é limitado. No entanto, não há restrições quanto ao financiamento governamental, e os governos na América

[27] Os termos CSIRT (Computer Security Incident Response Team) e CERT (Computer Emergency Response Team) são frequentemente usados de forma intercambiável, mas há diferenças sutis em suas origens e na forma como são representados.
[28] CERT.LU, About CERT.LU. Disponível em: https://www.cert.lu. Acesso em: 18 out. 2024.
[29] ENISA, Information Sharing and Analysis Centres (ISACs) Cooperative Models, 2017. Disponível em: https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models?v2=1.

Latina (LATAM) poderiam oferecer apoio financeiro conforme necessário, especialmente em situações de compartilhamento de informações sobre incidentes específicos. Esse modelo é amplamente adotado em países maiores, onde o setor privado é forte, com metas de cibersegurança bem definidas e orçamentos mais robustos para iniciativas de compartilhamento de informações. A seguir, alguns exemplos de ISACs setoriais:

» **Financial Services (FS-ISAC)** – Fundado em 1999, o FS-ISAC tem como objetivo promover a resiliência cibernética no sistema financeiro global, protegendo as instituições financeiras e os indivíduos que elas atendem. Embora tenha sede nos EUA, o FS-ISAC agora conta com membros em mais de 75 países, o que demonstra a flexibilidade e o alcance que um ISAC pode alcançar.[30]

» **Banking Cybersecurity Center (BCC)** – Polônia – Uma plataforma voltada para que os bancos se comuniquem e troquem informações sobre vulnerabilidades e ameaças relevantes. A adesão é aberta a qualquer banco comercial na Polônia.[31] O BCC é um exemplo de ISAC que combina tanto o foco setorial quanto o nacional.

Os ISACs setoriais também podem ser estruturados para permitir a participação internacional, ampliando seu alcance para além de um único país. No entanto, os ISACs internacionais enfrentam desafios relacionados à construção de confiança, que podem ser mais difíceis devido às diferenças culturais entre as partes envolvidas.[32] Abaixo, alguns exemplos:

» **EU FI-ISAC** – Criado em 2008, o ISAC de Instituições Financeiras da União Europeia foi desenvolvido para compartilhar informações sobre atividades cibercriminosas que afetam a comunidade financeira europeia. A adesão inclui representantes do setor financeiro de diversos países, CERTs nacionais, e agências de aplicação da lei. Também participam organizações como ENISA, Europol, o Banco Central Europeu (BCE), o Conselho Europeu de Pagamentos (EPC) e a Comissão Europeia. O EU FI-ISAC conta com o apoio ativo da ENISA.[33]

» **EE-ISAC** – O ISAC de Energia da Europa visa melhorar a resiliência e segurança da infraestrutura energética europeia, promovendo o compartilhamento de informações com base na confiança e possibilitando um esforço conjunto na análise de ameaças. Os membros incluem prestadores de serviços e técnicos, utilitários, acadêmicos, institutos de pesquisa, além de organizações governamentais e sem fins lucrativos.[34]

---

[30] FS-ISAC, What We Do. Disponível em: https://www.fsisac.com. Acesso em: 18 out. 2024.
[31] ENISA, ISACs Cooperative Models.
[32] ENISA, ISACs Cooperative Models.
[33] ENISA, European Financial Institutes – Information Sharing and Analysis Centre, A Public-Private Partnership. Disponível em: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/finance/european-fi-isac-a-public-private-partnership. Acesso em: 18 out. 2024.
[34] European Energy Information Sharing & Analysis Centre, Home. Disponível em: https://www.ee-isac.eu. Acesso em: 18 out. 2024.

PAPÉIS E RESPONSABILIDADES

Um ISAC é uma ferramenta eficaz para promover a cooperação público-privada, mas é essencial definir claramente os papéis e responsabilidades de todas as entidades envolvidas para garantir o bom funcionamento da organização. Dentro de um ISAC, existem três grupos principais: o "facilitador", os "membros" e os "parceiros". O facilitador tem um papel secretarial, responsável por organizar a logística do grupo, como definir a frequência das reuniões, recrutar novos membros e gerenciar a comunicação.[35] A maioria dos facilitadores também oferece a infraestrutura técnica e os processos necessários para o compartilhamento de informações, que podem variar desde ferramentas simples, como listas de e-mails, até plataformas avançadas para compartilhar e analisar indicadores de comprometimento (IOCs). Os membros são as entidades que ativamente compartilham e recebem informações, usufruindo dos benefícios da adesão e pagando as taxas correspondentes para participar. Os parceiros do ISAC, por sua vez, são especialistas no assunto e organizações que participam de sessões específicas, geralmente oferecendo conhecimentos especializados sobre temas particulares. Abaixo, detalhamos as atividades de cada parte envolvida em um ISAC. Vale ressaltar que a falta de clareza nos papéis e responsabilidades pode prejudicar o funcionamento adequado de um ISAC.

Setor Público

As instituições governamentais podem ter papéis variados dentro de um ISAC, dependendo da situação. Em alguns casos, o governo pode atuar como facilitador, oferecendo espaços para as reuniões e assumindo outras funções administrativas. Além disso, os governos podem fornecer financiamento direto para apoiar o desenvolvimento do ISAC. Em outros casos, o governo pode criar um marco legal que regule tanto o compartilhamento de informações quanto a formação de um ISAC.[36] O papel do setor público, porém, varia conforme a natureza da entidade envolvida. Por exemplo, as Agências Nacionais de Cibersegurança (NCAs) costumam participar de ISACs, seja facilitando a operação do ISAC ou participando ativamente do compartilhamento e análise de informações. Muitas NCAs também operam um CSIRT, que desempenha um papel essencial dentro do ISAC. É comum que uma ou duas entidades públicas estejam envolvidas em um ISAC, seja de maneira regular ou esporádica.

[35] ENISA, ISACs Cooperative Models.
[36] ENISA, ISACs Cooperative Models.

Agências de Aplicação da Lei e Comunidade de Inteligência

As agências de aplicação da lei e os serviços de inteligência podem ser parceiros importantes nos ISACs, devido às suas funções especializadas e ao acesso a informações cruciais. Nos EUA, as agências de aplicação da lei interagem regularmente com os ISACs, pois muitas das informações compartilhadas por elas não são classificadas de forma tradicional, embora também não sejam públicas. Por outro lado, as agências de inteligência tendem a limitar seu envolvimento com os ISACs, devido à natureza confidencial de suas informações. Mesmo assim, é fundamental manter uma conexão com essas comunidades, envolvendo-as como parceiras em sessões específicas de discussão e troca de conhecimentos.

Indústria e Proprietários de Infraestruturas Críticas e Operadores

A indústria deve ser a principal força motriz por trás de todos os ISACs, tanto como facilitadora quanto como membro. Mesmo com a presença de entidades públicas, é o setor privado que deve definir a forma e a funcionalidade da cooperação.[37] O setor privado é responsável pela maior parte da infraestrutura crítica, e à medida que a tecnologia e os serviços de infraestrutura crítica se tornam mais eficientes com a transformação digital, os proprietários e operadores de ativos dependem cada vez mais da segurança tanto da tecnologia da informação (TI) quanto da tecnologia operacional (OT). Isso faz da cibersegurança uma prioridade essencial para garantir a entrega segura dos serviços, a confiança pública e a continuidade dos negócios. Além disso, a participação de empresas da indústria deve incluir uma ampla gama de entidades, desde os proprietários e operadores de infraestrutura crítica até os fornecedores de tecnologia operacional, cujos produtos são essenciais para o funcionamento desses ativos.

Acadêmicos

Os ISACs frequentemente envolvem o meio acadêmico como parceiro, permitindo que o governo e a indústria comuniquem suas necessidades de pesquisa e desenvolvimento de forma clara.[38] A colaboração com instituições acadêmicas pode gerar novas soluções para setores críticos e para o cenário cibernético em geral. Além disso, serve como um fórum eficaz para que pesquisadores testem a viabilidade e os resultados de seus estudos na prática, recebendo feedback valioso dos proprietários e operadores de infraestrutura crítica.

---

[37] Ibid.
[38] ENISA, ISACs Cooperative Models.

GOVERNANÇA E FINANCIAMENTO

Por sua natureza flexível, os ISACs podem ser organizados de diversas maneiras. Alguns têm uma estrutura de governança bem definida, com papéis claros, como secretariado e conselho de gestão, enquanto outros funcionam de maneira mais informal, com voluntários responsáveis pela organização das reuniões. As atividades principais do ISAC, como reuniões e exercícios, são determinadas pela governança do grupo. Quanto mais estruturado for o ISAC, mais específicas serão as tarefas a serem realizadas. Em modelos com menos estrutura, o ISAC pode ser mais flexível e focar em casos especiais, conforme necessário. Ambos os modelos de governança são válidos e podem ser adaptados às necessidades dos membros do ISAC.

Abordagem de Governança Estruturada

A gestão de um ISAC pode seguir diferentes modelos. Em alguns casos, o grupo é liderado por um presidente e um vice-presidente, enquanto em outros a liderança é assumida por um conselho de gestão ou comitê diretor. Esses papéis de liderança geralmente não são eletivos e podem envolver tanto trabalho remunerado quanto voluntário, dependendo do tamanho e das necessidades do ISAC. Essas posições costumam ser ocupadas por membros ou organizações do setor privado que estão altamente comprometidos com o ISAC. Uma vez definidos, o principal objetivo dessas lideranças é criar um plano estratégico para orientar os objetivos da comunidade. Normalmente, essas estruturas incluem regras claras para eleições e definição de responsabilidades.[39]

Governança com Órgão de Apoio

Em outros casos, um ISAC pode designar uma única entidade para atuar como secretariado. Isso é mais comum quando o setor público está envolvido, pois a administração pública supervisiona as interações do grupo, garantindo que as atividades sigam uma agenda bem definida.

Governança Flexível

Alguns ISACs não possuem uma estrutura de governança bem definida nem papéis claramente estabelecidos, o que resulta em uma comunidade altamente flexível, geralmente liderada por voluntários. Em cada reunião, uma organização ou representante diferente se oferece para sediá-la, rotacionando a responsabilidade de forma contínua. Esses ISACs normalmente não contam com um plano de ação formal, e as decisões são tomadas de maneira improvisada, conforme os desafios vão surgindo. Nesse modelo flexível, as reuniões acontecem em diferentes locais, permitindo que a comunidade troque experiências e conheça as culturas de seus pares. Contudo, a falta de formalidade pode reduzir o engajamento dos stakeholders.

---

[39] Ibid.

Financiamento

Assim como a estrutura e a governança, existem diferentes formas de financiar um ISAC, algo que será relevante para a América Latina considerar à medida que formalizam o compartilhamento de informações na região.[40]

- **Taxas Obrigatórias** – Este é o modelo de financiamento mais comum para um ISAC. Os membros pagam taxas anuais, cujo valor varia de acordo com o tamanho da organização e seu nível de envolvimento.
- **Contribuições Voluntárias** – Nesse modelo, os membros contribuem financeiramente de forma voluntária, além de oferecerem recursos necessários, como espaços para reuniões, pessoal dedicado às atividades do ISAC, criação de grupos de trabalho, entre outros.
- **Subsídios Governamentais** – Embora pouco frequentes, subsídios do governo podem ser disponibilizados quando há programas ou marcos legais específicos. Esse tipo de financiamento geralmente cobre facilidades como gestão de secretariado ou disponibilização de espaços para reuniões. No entanto, o objetivo é incentivar a participação do setor privado, e não sustentar o ISAC a longo prazo.

PRINCIPAIS COMPETÊNCIAS

Esta seção destaca as principais competências que um ISAC pode oferecer aos seus membros:

Compartilhamento de Informações – O compartilhamento de informações é a principal função de um ISAC, permitindo que os membros troquem inteligência crítica para se defenderem coletivamente contra ameaças cibernéticas. Isso inclui:

- **Indicadores de ameaças**, como endereços IP maliciosos ou assinaturas de malware.
- **Detalhes sobre incidentes**, como técnicas de ataque, intenções e impactos.
- **Vulnerabilidades**, seja em softwares, hardwares ou processos de negócios.
- **Estratégias de mitigação**, como patches de segurança ou atualizações de antivírus.

Os membros também compartilham melhores práticas, que vão desde estratégias de resposta a incidentes até a implementação de controles de segurança. As informações são trocadas por meio de plataformas seguras, como portais web anônimos (ex.: MISP)[41], e-mails criptografados e reuniões presenciais. Ao facilitar o compartilhamento rápido e seguro desses dados, os ISACs ajudam as organizações a responderem de forma ágil às ameaças emergentes, aumentando sua

[40] ENISA, ISACs Cooperative Models.
[41] MISP Threat Sharing. Disponível em: https://www.misp-project.org. Acesso em: 23 out. 2024.

resiliência e reduzindo a probabilidade de incidentes cibernéticos em larga escala.
Reuniões Regulares e Grupos de Trabalho – Reuniões regulares e grupos de trabalho dedicados são fundamentais para manter a comunicação ativa e fortalecer a colaboração entre os membros do ISAC. Esses encontros reúnem especialistas da indústria e parceiros para discutir e enfrentar desafios urgentes de cibersegurança. Ao oferecer uma plataforma para o diálogo contínuo e a troca de conhecimentos, os ISACs promovem maior especialização e uma abordagem mais proativa na solução de problemas, garantindo que os membros estejam melhor preparados para enfrentar os riscos cibernéticos em constante evolução.

Conferências e Eventos Paralelos – Conferências e eventos paralelos ajudam a aumentar a visibilidade das atividades do ISAC e a envolver ainda mais as partes interessadas. Esses encontros permitem que os participantes se atualizem sobre novas tendências, avanços tecnológicos e estratégias de cibersegurança. Os eventos paralelos, como workshops, mesas-redondas e sessões de treinamento, oferecem espaços focados para discutir áreas específicas de interesse ou desafios do setor. Além disso, são ótimas oportunidades para networking e colaboração, ampliando a influência e o alcance do ISAC dentro da indústria. Esses eventos são essenciais para manter as partes interessadas bem-informadas e conectadas.

Exercícios – Os ISACs promovem exercícios para avaliar e melhorar a prontidão cibernética de seus membros. Esses exercícios podem incluir desde simulações para governança, que preparam os executivos para tomar decisões críticas, até treinamentos operacionais e técnicos que testam a capacidade das organizações de aplicar procedimentos e utilizar ferramentas de cibersegurança de maneira eficaz.[42] Eles são fundamentais para identificar vulnerabilidades, validar o nível de preparação e fortalecer a capacidade de resposta a incidentes em todos os níveis da organização.

Análise – A análise é um serviço de alto valor oferecido pelos ISACs, ajudando os membros a compreender e priorizar os riscos cibernéticos. Os ISACs realizam **análises de vulnerabilidades e ameaças**, aproveitando a expertise das organizações participantes, muitas vezes por meio de grupos de trabalho colaborativos. Essa abordagem permite a criação de insights aprofundados sobre ameaças emergentes, ajudando os membros a se anteciparem e mitigarem riscos de forma mais eficaz. Apesar de a análise detalhada exigir recursos significativos, os membros geralmente reconhecem sua importância e estão dispostos a investir nesse serviço.
Além disso, os ISACs oferecem conhecimentos essenciais sobre questões legais e regulatórias relacionadas ao compartilhamento de informações. Entender o cenário legal é crucial, pois leis de privacidade e obrigações regulatórias, como a comunicação obrigatória de incidentes, podem tanto criar obstáculos quanto gerar novas demandas para um compartilhamento

[42] ENISA, Cross-Sector Exercise Requirements, March 2022, file:///C:/Users/acs07/Downloads/Cross-sector%20exercise%20requirements%20(1).pdf.

eficiente de dados. Os ISACs orientam sobre como compartilhar informações de forma que esteja em conformidade com essas regulamentações, proporcionando segurança aos membros e incentivando um intercâmbio mais aberto de dados.

Para ISACs que não possuem uma equipe dedicada à análise, a tarefa de fornecer uma análise consistente de ameaças pode ser desafiadora, especialmente com grandes volumes de dados que exigem tempo e recursos consideráveis. Nesse caso, a colaboração com agências governamentais – como a ENISA em iniciativas pan-europeias – pode ajudar a fortalecer a capacidade analítica dos ISACs.[43]

Construção de confiança – A confiança é a base de qualquer ISAC eficaz. Ao promover interações frequentes, os ISACs incentivam a comunicação aberta e a colaboração entre os membros. Construir relacionamentos pessoais e estabelecer mecanismos formais, como acordos de confidencialidade, códigos de conduta, o uso de regras de Chatham House e o Traffic Light Protocol (TLP), garante que os membros se sintam seguros ao compartilhar informações sensíveis. A confiança fortalece a eficácia do compartilhamento de dados, tornando o ISAC mais resiliente e confiável.

[43] ENISA, ISACs Cooperative Models.

Avaliando a Necessidade de um ISAC para a LATAM

A América Latina é uma região fortemente ameaçada por ciberataques, devido a características locais que funcionam como "aceleradores", como o uso generalizado de software não-licenciados, altas taxas de pirataria e a rápida digitalização dos mercados financeiros, incluindo o crescimento de diversas empresas fintech.[44] As grandes lacunas de maturidade nas capacidades de resposta a incidentes e cibersegurança entre os países da LATAM tornam a região um alvo prioritário para agentes de ameaças, com alguns países enfrentando mais de 1.000 ciberataques por segundo.[45] Em 2024, o mercado de cibersegurança na América Latina foi avaliado em 8,92 bilhões de dólares, com a expectativa de que esse valor ultrapasse 12,48 bilhões de dólares até 2029.[46] O aumento das ameaças cibernéticas na região evidencia a necessidade urgente de melhorar o compartilhamento formalizado de informações. Esta seção analisa como a criação de ISACs na LATAM pode fortalecer a resposta às ameaças e alinhar-se com as metas políticas relacionadas à governança digital, à colaboração multissetorial e ao desenvolvimento de força de trabalho.

A criação de ISACs na LATAM pode fortalecer a resposta às ameaças e alinhar-se com as metas políticas relacionadas à governança digital, à colaboração multissetorial e ao desenvolvimento de força de trabalho.

CENÁRIO DE AMEAÇAS

A região da LATAM é altamente interconectada, o que significa que os ciberataques podem afetar entidades muito além do alvo inicial, tornando a resiliência regional ainda mais importante. Alguns países da LATAM já estão começando a adotar as ações proativas de outros. Por exemplo, após a série de ataques de ransomware que afetaram a Costa Rica em 2023, El Salvador tomou medidas para desenvolver um programa robusto de cibersegurança e atualizar suas políticas para evitar problemas semelhantes.[47] Um ISAC forneceria um método formalizado para compartilhar as lições aprendidas e facilitar o desenvolvimento de políticas nacionais de cibersegurança mais eficazes em toda a região.

---

[44] Americas Quarterly, How Latin America's Governments Compare on Anti-Piracy, January 17, 2019. Disponível em: https://www.americasquarterly.org/article/how-latin-americas-governments-compare-on-anti-piracy/.
[45] Jamaica Major Organized Crime and Corruption Agency, Combatting Cyber Crime. Disponível em: https://www.moca.gov.jm/cyber-crime. Acesso em: 25 jul. 2024.
[46] Mordor Intelligence, Latin America Cybersecurity Market Size (2024-2029). Disponível em: https://www.mordorintelligence.com/industry-reports/latin-america-cyber-security-market/market-size. Acesso em: 25 jul. 2024.
[47] Telecommunications Industry Association, Costa Rica Takes Bold and Decisive Stance on Cybersecurity, Sept. 6, 2023. Disponível em: https://tiaonline.org/press-release/costa-rica-takes-bold-and-decisive-stance-on-cybersecurity/.

Atualmente, a LATAM depende de países que estão ativamente envolvidos no compartilhamento de informações para obter assistência em resposta a incidentes, financiamento e orientação no desenvolvimento de estratégias cibernéticas. Quando ocorrem incidentes cibernéticos, os países que fazem parte de redes formalizadas de compartilhamento de informações estão em uma posição mais favorável para responder e se recuperar de ataques. Por exemplo, os EUA têm a rede de ISACs mais robusta do mundo e lideram o índice global de cibersegurança com pontuação 100.[48] Quando a Costa Rica foi alvo de um ataque de ransomware devastador, que lhe custou cerca de 30 milhões de dólares por dia, os EUA, Israel e Espanha intervieram. Esses países, participantes de ISACs cibernéticos, estavam preparados para ajudar a Costa Rica, em parte graças aos recursos e conhecimentos adquiridos por meio do compartilhamento de informações.[49] Assim, investir na criação de ISACs na LATAM fortalecerá a resiliência regional e reduzirá a dependência da região em relação a parceiros externos.

Não compartilhar informações pode ser mais arriscado do que os próprios riscos do compartilhamento, pois muitos hackers já operam compartilhando suas estratégias entre si para obter maior vantagem.[50] Assim, participar de um ISAC ajuda a nivelar o campo de jogo contra esses atores maliciosos que já estão trocando informações. Embora construir confiança seja um desafio, também representa uma oportunidade para maior unidade regional. Os participantes do ISAC podem alertar proativamente seus pares sobre ameaças em andamento e aprender com as experiências compartilhadas. Embora a construção de confiança seja um processo contínuo, o sucesso dos ISACs em outras partes do mundo mostra o grande potencial dessa abordagem para fortalecer a resiliência cibernética regional.

ALINHAMENTO POLÍTICO

O desenvolvimento de ISACs na LATAM está em sintonia com o crescente foco da região em governança digital. Vários países começaram a criar Estratégias Nacionais de Cibersegurança ou a propor legislações para estabelecer uma Agência Nacional de Segurança Digital, com o compartilhamento de informações e uma maior colaboração multissetorial como iniciativas principais. Por exemplo, o Chile implementou uma nova política nacional de cibersegurança em março de 2024, chamada "Lei Chilena de Cibersegurança e Infraestrutura Crítica".[51] Considerada uma lei inovadora na LATAM, seu objetivo é promover a gestão de riscos,

[48] ITU Publication, Global Cybersecurity Index.
[49] Cytek Security, Enhancing the National Security Posture of Costa Rica with an Integrated Approach, Jan. 9, 2024. Disponível em: https://cytek-security.com/resources/enhancing-the-national-security-posture-in-costa-rica-with-an-integrated-approach/.
[50] Computer Security Online, What is an ISAC or ISAO?, July 26, 2022. Disponível em: https://www.csoonline.com/article/567485/what-is-an-isac-or-isao-how-these-cyber-threat-information-sharing-organizations-improve-security.html.
[51] National Cybersecurity Coordination, Chilean Government Enacts Cybersecurity Law, Mar. 26, 2024. Disponível em: https://ciberseguridad.gob.cl/en/news/chile-enacts-cybersecurity-law-creates-cybersecurity-agency/#:~:text=The%20digital%20security%20of%20Chileans,cybersecurity%20actions%20of%20State%20agencies.

implementar padrões de segurança para aprimorar a prevenção, incluindo respostas a ciberataques por meio de parcerias público-privadas (PPPs), e estabelecer obrigações de cibersegurança, com sanções para quem não cumprir. A lei também criou um CSIRT Nacional e um Conselho Multissetorial, abrangendo todas as organizações, públicas ou privadas, que prestem serviços que impactem a infraestrutura crítica. Um ISAC, por definição, envolve o compartilhamento de informações entre entidades públicas e privadas, o uso de engajamento multissetorial e o intercâmbio de dados sobre ameaças e respostas a incidentes cibernéticos relacionados à infraestrutura crítica. Esses três aspectos estão presentes na Lei Chilena, mas são implementados de maneiras descentralizadas. Criar um ISAC ajudaria a atender diretamente às metas da lei e unificaria sua execução, facilitando o acompanhamento dos avanços.[52]

O México tem se empenhado em aumentar a coordenação e o intercâmbio de informações, e em agosto de 2022, o país, em parceria com os EUA, estabeleceu um "Grupo de Trabalho sobre Questões Cibernéticas" para promover um "compromisso compartilhado com uma internet aberta, interoperável, segura e confiável, além de um ciberespaço estável".[53]

Uma das principais iniciativas desse grupo foi fortalecer os mecanismos de coordenação técnica para enfrentar as ameaças cibernéticas. Esse é o objetivo central de um ISAC, o que demonstra como a criação de um ISAC na LATAM se alinha perfeitamente aos esforços já em andamento na região. Além disso, especialistas da indústria no Brasil recentemente sugeriram a criação de uma Agência Nacional de Segurança Digital para centralizar recursos e permitir a implementação da Estratégia Nacional de Cibersegurança do país. A agência manteria a cibersegurança como uma das prioridades principais do governo, o que é crucial, já que o Brasil é o segundo país mais vulnerável a ciberataques no mundo.[54]

É importante destacar que as políticas variam bastante em seu desenvolvimento, criando lacunas significativas na prontidão cibernética em toda a LATAM. De acordo com o GCI (Índice Global de Cibersegurança da UIT), o México obteve uma pontuação de 81,75 em prontidão cibernética, enquanto Honduras teve apenas 2,2.[55] A diferença na prontidão cibernética é consideravelmente maior na LATAM do que em outras regiões do mundo, o que indica que o aprimoramento do compartilhamento de informações pode gerar resultados significativos para os países

---

[52] Lexology, Stepping up in Latin America: Chile enacts a new Cybersecurity Law. Disponível em: https://www.lexology.com/library/detail.aspx?g=82a52636-a23c-4b8b-9158-3203f69a3fb0#:~:text=Chile%20has%20also%20approved%20its,legislation%20and%20regulation%20in%20Chile. Acesso em: 25 jul. 2024.
[53] Carnegie Endowment for International Peace, Mexico's National Cybersecurity Policy: Progress Has Stalled Under AMLO, May 28, 2024. Disponível em: https://carnegieendowment.org/research/2024/05/mexicos-national-cybersecurity-policy-progress-has-stalled-under-amlo?lang=en&er=russia-eurasia.
[54] Center for Cybersecurity Policy and Law, Hearing Highlights Industry Calls for Brazilian National Digital Security Agency, July 16, 2024. Disponível em: https://www.centerforcybersecuritypolicy.org/insights-and-research/hearing-highlights-industry-calls-for-brazilian-national-digital-security-agency.
[55] ITU Publications, Global Cybersecurity Index 2020. Disponível em: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E. Acesso em: 24 jul. 2024.

da região que estão mais atrasados nesse aspecto.[56] Um ISAC pode ajudar a preencher essa lacuna de maturidade entre os países da LATAM, compartilhando lições aprendidas e incentivando os países menores a adotar medidas proativas para proteger seus sistemas.

COLABORAÇÃO MULTISSETORIAL

Os ISACs estão claramente alinhados com as iniciativas globais de compartilhamento de informações e parcerias público-privadas (PPPs). Em 2022, 99 países assinaram ou ratificaram um acordo multilateral sobre compartilhamento de informações, e mais de 140 países participaram de atividades internacionais, como conferências de cibersegurança, workshops, parcerias e convenções com outros países.[57] Além disso, 86 países se envolveram em PPPs internacionais ou domésticas, e 62 países participaram de ambos.[58] O compartilhamento de informações tem demonstrado seu valor em nível global, com governos de todo o mundo comprometidos em ampliar sua participação em PPPs e mecanismos de compartilhamento de informações. Por exemplo, uma análise da economia digital da Jamaica, realizada pelo Fórum do Banco Mundial, revelou que a falta de compartilhamento de informações com o setor privado estava enfraquecendo a arquitetura de cibersegurança do país. A pesquisa apontou que a "ausência de fóruns formais e canais de comunicação para cooperação, visando aumentar a confiança digital e o conhecimento compartilhado limitado", estava limitando a resiliência cibernética da Jamaica.[59] Portanto, um ISAC na LATAM está em sintonia com o movimento global em direção a um maior compartilhamento de informações e pode fortalecer a resiliência dos países da região que ainda estão mal preparados em termos de cibersegurança.

Os esforços atuais de compartilhamento de informações na LATAM (que serão detalhados abaixo) não podem ser considerados mecanismos formais como um ISAC, pois não envolvem todas as partes interessadas relevantes e frequentemente limitam a participação a contraparte do governo em nível nacional. Além disso, não existe uma plataforma centralizada única para conectar as diversas iniciativas mencionadas. A Rede de CSIRTs das Américas da OEA ilustra bem esse problema, já que a participação é restrita a outros CSIRTs governamentais, sem incluir o setor privado ou a academia.[60] Outro exemplo é o Fórum de Equipes de Segurança e Resposta a Incidentes (FIRST), que busca unir equipes de segurança e resposta a incidentes na região, adotando um modelo de governança baseado em uma rede de

[56] ITU Publications, Global Cybersecurity Index.
[57] ITU Publications, Global Cybersecurity Index.
[58] ITU Publications, Global Cybersecurity Index.
[59] The World Bank, Digital Economy for Latin America and the Caribbean Country Diagnostic: Jamaica, pg. 153, April 2024. Disponível em: https://thedocs.worldbank.org/en/doc/61714f214ed04bcd6e9623ad0e215897-0400012021/related/IDU1c6883bf81f279148581a6dd184a5f721a2ea.pdf.
[60] CSIRT Americas. Disponível em: https://csirtamericas.org/en. Acesso em: 24 jul. 2024.

pares de CSIRTs.[61] O progresso na criação de CSIRTs nacionais é extremamente positivo e gerou uma quantidade considerável de inteligência cibernética de diversos fornecedores. No entanto, essa informação ou não está acessível para a maioria das organizações, por estarem fora dos esforços de intercâmbio de informações atuais, ou as organizações simplesmente não possuem a maturidade ou os mecanismos necessários para processar e compreender as informações sobre ameaças que foram coletadas.

Limitar a participação nos esforços de compartilhamento de informações só vai reduzir ainda mais a capacidade da LATAM de combater o aumento dos ciberataques. Como região, é fundamental que, quando ocorrerem incidentes, todos os setores tenham acesso às informações relevantes. Um ISAC na LATAM preencheria essa lacuna, envolvendo partes interessadas do setor privado e da academia no intercâmbio de informações sobre ameaças e melhores práticas, criando um ambiente coeso em que todas as partes relevantes estão incluídas. Os ISACs também permitem que atores menos maduros, como pequenas e médias empresas, compreendam e implementem as informações compartilhadas. Sem um centro centralizado para o compartilhamento de informações, muitos dos recursos nos quais os países da LATAM estão investindo tempo e dinheiro podem não ser totalmente aproveitados, já que a participação é limitada. Um ISAC dedicado à LATAM também garantiria que as informações compartilhadas tivessem o contexto específico da região, em vez de depender de parceiros internacionais que não têm o mesmo conhecimento dos problemas locais para fortalecer a cibersegurança.[62]

ATRAÇÃO DE TALENTOS E OPORTUNIDADES EDUCACIONAIS

Os benefícios do compartilhamento de informações vão além da resposta a incidentes: um ISAC na LATAM poderia ser um ponto de partida para atrair e reter talentos cibernéticos, ao mesmo tempo em que promove uma comunidade mais consciente sobre cibersegurança. A região enfrenta grandes disparidades no acesso à internet, o que dificulta a construção de uma força de trabalho cibernética robusta. Embora tenha havido algum progresso na criação de iniciativas educacionais em cibersegurança, elas ainda são fragmentadas, com a maioria dos esforços concentrados em áreas específicas. Mais de 1.600 universidades na região oferecem programas de graduação e pós-graduação em tecnologias digitais, mas esses cursos estão limitados a países como Argentina, Brasil, Chile, Colômbia, México, Peru, Equador, Costa Rica e Uruguai.[63] Além disso, dentro desses países, a Argentina concentra 66% das universidades que oferecem tais cursos.

---

[61] FIRST, Vision and Mission Statement. Disponível em: https://www.first.org/about/mission. Acesso em: 26 jul. 2024.
[62] Trade EC Europa, Cybersecurity Sector in Central America, Novembro de 2022, https://trade.ec.europa.eu/access-to-markets/en/country-assets/euca_05_Cybersecurity%20sector%20in%20Central%20America.pdf.
[63] CEPAL, Latin American Economic Outlook 2020: Digital transformation for building back better, September 9, 2020, pg. 105.

Educar o público da LATAM sobre iniciativas cibernéticas, oportunidades e habilidades básicas pode criar empregos para cerca de 60% dos trabalhadores da região que estão no setor informal.[64] No entanto, isso exigirá maior conectividade digital e educação para expandir a força de trabalho cibernética. Uma pesquisa da CEPAL de 2020 revelou que 75% das áreas mais ricas da América Latina e do Caribe tinham acesso à internet, enquanto apenas 37% da população mais pobre tinha essa conexão.[65] Vários países começaram a oferecer treinamentos online gratuitos em habilidades digitais, como o Plano de Desenvolvimento de Habilidades Digitais "O IFT te ensina", os Centros de Transformação Digital Empresarial na Colômbia e os Infocentros Comunitários no Equador. No Brasil, iniciativas como a Rede Nacional de Pesquisa e Educação (RNP), o SENAI-SP e a Softex criaram o curso gratuito de cibersegurança "Hackers do Bem", voltado para quem deseja trabalhar na área.[66] No entanto, esses esforços ainda são dispersos, e a LATAM carece de recursos regionais abrangentes para melhorar a alfabetização digital.[67] Para promover mudanças significativas, as oportunidades educacionais precisam alcançar um público mais amplo e aumentar a conscientização em toda a região. Como um centro de colaboração entre acadêmicos, autoridades governamentais e organizações do setor privado, um ISAC pode expandir o trabalho já realizado, unificando a educação e atraindo talentos para a força de trabalho cibernética. Os ISACs oferecem uma oportunidade única para atender às necessidades específicas da América Latina e do Caribe, superando o simples compartilhamento de informações e facilitando outras iniciativas, como o desenvolvimento educacional e da força de trabalho.

[64] CEPAL, Latin American Economic Outlook 2020: Digital transformation for building back better, September 9, 2020.
[65] The World Bank, The Digital Economy Initiative for Latin America and the Caribbean, April 2024. Disponível em: https://www.worldbank.org/en/programs/de4lac.
[66] Hackers do Bem. Disponível em: https://hackersdobem.org.br/o-programa.
[67] CEPAL, Latin American Economic Outlook 2020: Digital transformation for building back better, September 9, 2020, pg. 108.

INICIATIVAS ATUAIS DE COMPARTILHAMENTO DE INFORMAÇÕES

Vários países da LATAM já iniciaram esforços para promover o compartilhamento de informações, embora a maioria dessas iniciativas ainda seja nacional. Embora alguns tenham começado a incluir o setor privado, muitas dessas ações ainda não têm a formalidade e o envolvimento amplo de um ISAC real. Esta seção apresenta uma visão geral das principais iniciativas em andamento na região.

Rede Federal de Gestão de Incidentes Cibernéticos do Brasil – No Brasil, as instituições do governo federal são obrigadas a participar da Rede Federal de Gestão de Incidentes Cibernéticos, que facilita o compartilhamento de informações sobre ameaças, incidentes e vulnerabilidades.[68] Empresas públicas e de capital misto, assim como suas subsidiárias, podem aderir à rede de forma voluntária.[69] Embora a rede seja aberta às empresas públicas, seu foco principal é promover a troca de informações entre as instituições públicas federais. No entanto, o Brasil conta com outros mecanismos alternativos. Por exemplo, no setor de telecomunicações, a Anatel criou um grupo de trabalho que utiliza uma plataforma de compartilhamento de informações sobre malware (MISP) para divulgar dados sobre ameaças e vulnerabilidades.[70] Além disso, organizações do setor financeiro, como a Federação Brasileira de Bancos, participam de redes internacionais de compartilhamento de informações, como a Financial Services Information Sharing and Analysis Network (FS-ISAC). O setor financeiro tem destacado que o compartilhamento de informações entre todos os setores de infraestrutura crítica poderia ser mais eficiente e automatizado, utilizando plataformas como o MISP, por exemplo.[71]

Belize – Países menores da LATAM, como Belize, também têm dado passos importantes para melhorar o compartilhamento de informações. Belize lançou sua Estratégia de Cibersegurança 2020–2030, que estabelece como prioridade o "desenvolvimento de uma capacidade nacional para resposta a incidentes e proteção de infraestrutura crítica de informações."[72] Dentro dessa prioridade, Belize planeja criar um diálogo com os setores-chave, adotando uma "abordagem faseada para implementar um protocolo de compartilhamento de informações."[73] Um ISAC regional complementaria essas iniciativas e ajudaria a fortalecer a resiliência cibernética na região.

---

[68] Global Cybersecurity Capacity Center, Cyber Capacity Review - Brazil, p. 46, Aug. 2023. Disponível em: https://www.gov.br/gsi/pt-br/ssic/eventos/CMMreportBrazil2023_finalversoemingls.pdf.
[69] Brazilian-American Chamber of Congress, Brazil creates cyber-attack response network, Jul 27, 2021. Disponível em: https://brazilcham.com/brazil-creates-cyberattack-response-network/.
[70] Global Cybersecurity Capacity Center, Cyber Capacity Review - Brazil.
[71] Ibid.
[72] Government of Belize, National Cybersecurity Strategy Towards a Secure Cyberspace 2020-2030, pg. 27. Disponível em: https://www.pressoffice.gov.bz/wp-content/uploads/2019/12/belize-cybersecurity-strategy-2020-2023.pdf. Acesso em: 25 jul. 2024.
[73] Ibid.

Rede CSIRT das Américas – A Organização dos Estados Americanos (OEA) coordena a Rede CSIRT das Américas, uma rede regional de equipes de resposta a incidentes de segurança cibernética (CSIRT) que facilita o compartilhamento de informações sobre ameaças, oferece assistência técnica para fortalecer os serviços CSIRT e promove treinamento para especialistas em cibersegurança.[74] A Rede CSIRT das Américas reflete o compromisso dos governos da região com o compartilhamento de informações e serve como um exemplo importante para a colaboração na área. Embora a rede seja focada principalmente nos CSIRTs da região, ela também envolve parceiros do setor privado que contribuem para as atividades do grupo.

CSIRT Financiero (Asobancaria) – O CSIRT Financiero, liderado pela Associação de Bancos e Instituições Financeiras da Colômbia (Asobancaria), é uma entidade sem fins lucrativos que representa o setor financeiro colombiano. O CSIRT apoia as instituições financeiras no enfrentamento de riscos cibernéticos por meio do compartilhamento de informações e da colaboração com organizações nacionais e internacionais.[75] Seu objetivo é ser o ponto central para o intercâmbio de informações sobre ameaças cibernéticas no setor financeiro, baseando-se na confiança mútua, e também atuar como um centro de pesquisa e inovação para melhorar a prevenção de ameaças. Essa iniciativa tem grande potencial para se tornar um ISAC oficial para o setor financeiro em toda a América Latina e o Caribe, envolvendo não só a Colômbia, mas toda a região.

República Dominicana "Cyber Drill" – No verão de 2023, a República Dominicana realizou seu "Cyber Drill" anual, reunindo diversas organizações da região e outros participantes internacionais dos EUA e Canadá.[76] O evento funcionou de forma semelhante a uma sessão presencial de ISAC, com o objetivo de "oferecer um espaço para analisar e discutir as necessidades, ações e iniciativas nacionais, além de promover o desenvolvimento de capacidades por meio de laboratórios de simulação de incidentes cibernéticos, visando proteger as infraestruturas críticas nacionais e a cibersegurança da região." Governos, instituições e CIRTs/CERTs nacionais colaboraram com técnicos e representantes de cibersegurança, e as sessões de compartilhamento criaram uma plataforma para cooperação e debates sobre segurança cibernética.[77]

FIRST – O Forum of Incident Response and Security Teams é uma organização globalmente reconhecida e líder em resposta a incidentes. O FIRST reúne uma ampla variedade de equipes de segurança e resposta a incidentes de setores governamentais, empresariais e acadêmicos. O objetivo do FIRST é promover a cooperação e a coordenação na prevenção de incidentes, incentivar respostas rápidas e fomentar o compartilhamento de informações

[74] CSIRT Americas. Disponível em: https://csirtamericas.org/en. Acesso em: 24 jul. 2024.
[75] CSIRT Asobancaria. Disponível em: https://www.csirtasobancaria.com/quienes-somos. Acesso em: 28 out. 2024.
[76] ITU Publications, Cyberdrill for Americas-Dominican Republic 2023, June 19, 2023. Disponível em: https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Pages/EVENTS/2023/cyberdrill-23-Dominican-Republic.aspx#gsc.tab=0.
[77] ITU Publications, Cyberdrill for Americas-Dominican Republic 2023.

entre seus membros e a comunidade em geral.[78] Atualmente, o FIRST conta com mais de 700 membros em regiões como África, Américas, Ásia, Europa e Oceania. Embora o FIRST não seja voltado exclusivamente para a LATAM, sua extensa rede de membros pode ser aproveitada para iniciativas futuras de compartilhamento de informações focadas na região.

FEBRABAN – Fundada em 1967, a Federação Brasileira de Bancos (FEBRABAN) é uma associação sem fins lucrativos que trabalha com diversas partes interessadas para promover o desenvolvimento econômico, social e sustentável do Brasil.[79] Em 2020, foi criado o Laboratório de Cibersegurança da FEBRABAN, com o objetivo de facilitar a colaboração entre as equipes de bancos associados, focando na prevenção, identificação e combate ao cibercrime. Essa iniciativa pode servir como um ponto de partida importante para melhorar a cooperação e o compartilhamento de informações no setor financeiro da região.

LACNIC – O Registro de Endereços de Internet para a América Latina e Caribe (LACNIC) é uma organização internacional não governamental, criada no Uruguai em 2002. Sua missão é gerenciar os recursos digitais da internet na região, mantendo altos padrões de excelência e transparência, além de promover um modelo participativo no desenvolvimento de políticas. O LACNIC lidera a construção da comunidade regional, fortalecendo as capacidades tecnológicas e a pesquisa aplicada para o desenvolvimento de uma internet estável e aberta.[80] A organização é gerida por um conselho de sete membros eleitos pelos seus membros, que somam mais de 12.500 entidades operando em 33 territórios da LATAM. O LACNIC também gerencia um CSIRT, que desempenha as "funções de coordenação necessárias para fortalecer as capacidades de resposta a incidentes relacionados aos recursos de numeração da Internet (Ipv4, Ipv6), Números Autônomos e Resolução Reversa na América Latina e no Caribe, com base nos objetivos específicos definidos pela missão do LACNIC, visando o fortalecimento contínuo de uma internet segura, estável, aberta e em crescimento."[81]

78 FIRST. Disponível em: https://www.first.org. Acesso em: 28 out. 2024.
79 FEBRABAN. Disponível em: https://portal.febraban.org.br/paginas/10/pt-br/#. Acesso em: 27 nov. 2024.
80 LACNIC. Disponível em: https://www.lacnic.net/966/1/lacnic/acerca-de-lacnic. Acesso em: 28 out. 2024.
81 CSIRT LACNIC. Disponível em: https://csirt.lacnic.net/acerca. Acesso em: 28 out. 2024.

Conclusão

A fragmentação das iniciativas de compartilhamento de informações na América Latina destaca a necessidade urgente de um ISAC regional centralizado para enfrentar as ameaças cibernéticas em constante evolução. Dada a vulnerabilidade da região a ciberataques, a criação de um ISAC representaria uma grande oportunidade para fortalecer a resiliência cibernética e a alfabetização digital, além de facilitar a colaboração com ISACs existentes e parceiros internacionais. Atualmente, a maioria dos países da LATAM depende de apoio mútuo e assistência de parceiros externos para responder a ameaças cibernéticas. Além disso, a resposta a incidentes na região varia consideravelmente, com alguns países contando com mecanismos mais avançados que outros. Estabelecer um ISAC para a LATAM ajudaria a otimizar a resposta a incidentes, criando uma rede segura e confiável onde os países poderiam compartilhar informações atualizadas sobre ameaças, melhores práticas e outros dados relevantes. Com o tempo, o ISAC também contribuiria para aumentar o conhecimento geral sobre cibersegurança em toda a região.

Os ISACs têm mostrado sua eficácia globalmente, com os países mais preparados sendo aqueles que participam dessas iniciativas. Um ISAC para a LATAM ajudaria a reduzir a dependência de aliados externos, como os EUA e a UE, ao fortalecer as capacidades locais de resposta a incidentes. Já há um interesse por uma iniciativa desse tipo, com esforços preliminares de compartilhamento de informações em andamento. As redes existentes de CSIRTs e a colaboração com ISACs mais maduros podem servir como modelos valiosos para a criação de um ISAC na LATAM, envolvendo stakeholders da indústria e da academia para garantir uma visão ampla das informações sobre ameaças.

Para maximizar sua eficácia, a LATAM deve considerar cuidadosamente os diferentes modelos de estrutura e governança de um ISAC. Dado os diferentes níveis de maturidade, uma abordagem híbrida pode ser mais adequada para a região. A LATAM pode começar com um modelo baseado em setores, como o financeiro, mais avançados, enquanto expande as iniciativas já existentes em nível nacional. Organizações da região que já participam de ISACs nos EUA ou na UE podem usar sua experiência para orientar o desenvolvimento dos ISACs na LATAM. Essas organizações têm um papel importante no fomento à colaboração, compartilhamento de conhecimento e fortalecimento de capacidades à medida que novos ISACs regionais são criados. Um ISAC específico para a LATAM poderia fornecer análises e insights mais locais, abordando ameaças, vulnerabilidades e tendências próprias da região, que podem não ser totalmente capturadas por ISACs globais. Esse foco regional permitiria uma análise de inteligência de ameaças mais precisa e estratégias de resposta mais adaptadas.
Construir relacionamentos pessoais será crucial para estabelecer confiança entre os participantes, e é importante garantir que recursos adequados sejam alocados para definir claramente papéis e responsabilidades, permitindo a produção de análises significativas.

ISACs existem globalmente e têm um histórico comprovado de eficácia no fortalecimento da resiliência em cibersegurança. Eles integram todos os stakeholders relevantes e podem ajudar a reduzir as lacunas de maturidade entre os diversos países da LATAM. Embora já existam esforços para melhorar o compartilhamento de informações na região, eles precisam de mais recursos e precisam ser ampliados para incluir todos os envolvidos. Dadas as grandes lacunas nas políticas de cibersegurança, treinamento digital e educação na LATAM, os ISACs podem trazer grandes benefícios para a região. Em particular, eles podem fornecer acesso a lições aprendidas e inteligência de ameaças acionável para entidades menos maduras, além de reforçar a resiliência coletiva da região diante das crescentes ameaças cibernéticas.

DIGI AMERICAS ALLIANCE MEMBERS

aws Apple CHECK POINT CISCO CLOUDFLARE CROWDSTRIKE fluid attacks we hack your software Google

kriptos LUMU METABASE Q netskope paloalto NETWORKS Resecurity

Santander Schneider Electric Telefónica tenable Trellix TREND MICRO

DIGI AMERICAS