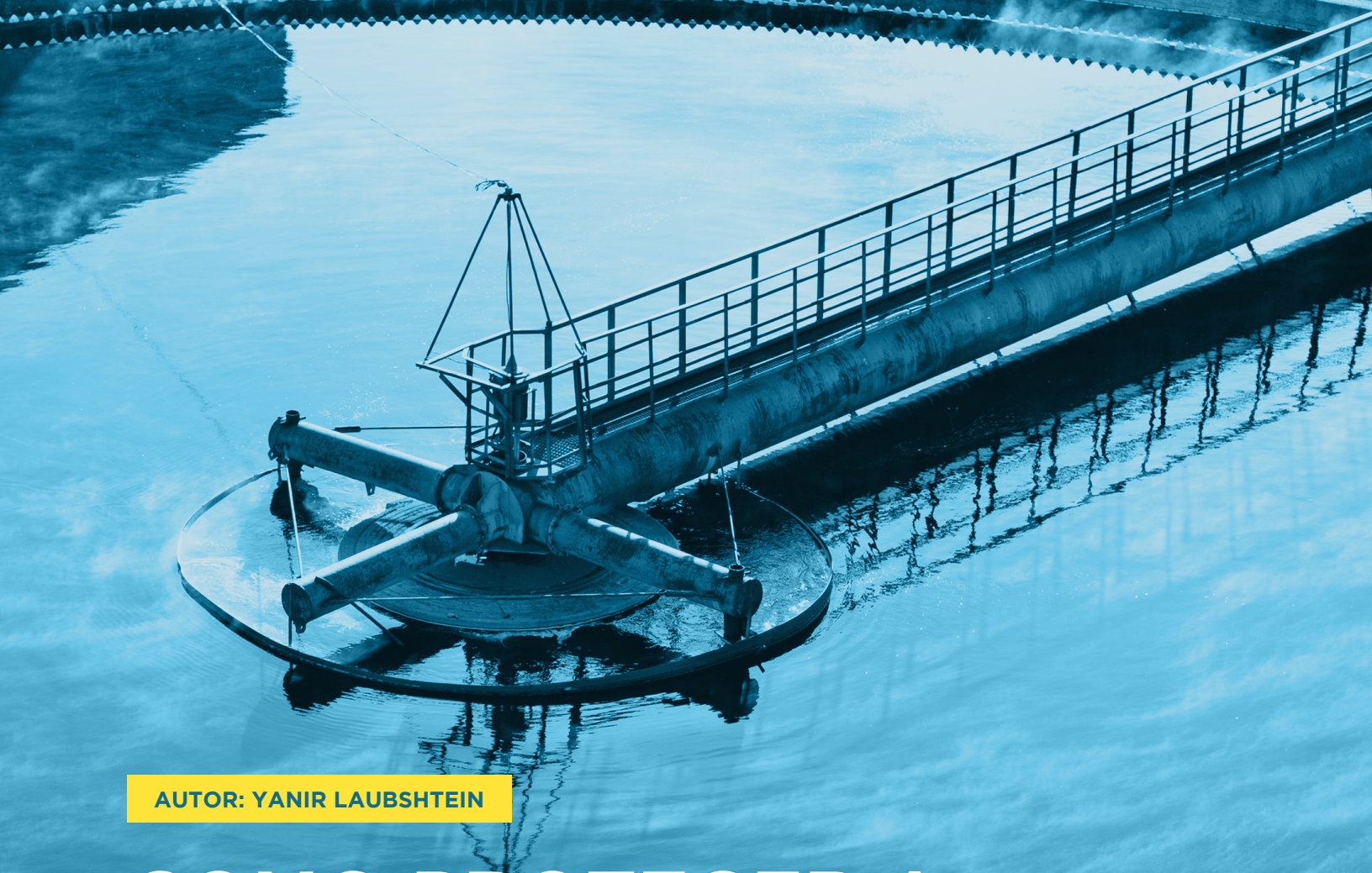


AUTOR: YANIR LAUBSHTEIN

COMO PROTEGER A INFRAESTRUTURA DE ÁGUA E SANEAMENTO CONTRA AMEAÇAS CIBERNÉTICAS

UM ESTUDO DE CIBERSEGURANÇA PARA A AMÉRICA LATINA E O CARIBE

EDITORES:
ARIEL NOWERSZTERN • MARCELLO BASANI • FERNANDO MELEAN • HILA COHEN MIZRAV

BID BID | LAB

Como proteger a infraestrutura de água e saneamento contra ameaças cibernéticas

Um estudo de cibersegurança
para a América Latina e o Caribe

Autor:
Yanir Laubshtein

Editores:
Ariel Nowersztern
Marcello Basani
Fernando Melean
Hila Cohen Mizrav

BID

COM A COLABORAÇÃO DE

SOURCE OF INNOVATION

Esta publicação faz parte da Source of Innovation, uma parceria promovida e cofinanciada pela Divisão de Água e Saneamento do Banco Interamericano de Desenvolvimento (BID) e pelo BID Lab, em coordenação com parceiros-chave como o governo da Suíça, por meio da Secretaria de Estado de Assuntos Econômicos (SECO), a Fundação FEMSA, o governo da Coreia, por meio do Ministério do Meio Ambiente, e o governo de Israel.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Economic Affairs SECO

Fundación FEMSA

Ministry of Economy and Industry of Israel
Foreign Trade Administration

Ministry of Environment
Republic of Korea

BID

BID | LAB

Códigos JEL:
H12, K24, L95, M15, N56, O32, O33, Q25.

Palavras-chave:
Água; saneamento; águas residuais; tratamento de águas; infraestruturas críticas; tecnologia operacional; sistemas de controle industrial; indústria 4.0; cibersegurança; políticas cibernéticas; ciberespaço; ciberataques; ameaças cibernéticas; resposta a incidentes; planejamento estratégico; proteção de dados.

Copyright © 2023 Banco Interamericano de Desenvolvimento (BID). Esta obra está licenciada sob uma licença Creative Commons CC BY 3.0 IGO (https://creativecommons.org/licenses/by/3.0/igo/legalcode). Os termos e condições indicados no link da URL devem ser atendidos e o respectivo reconhecimento deve ser concedido ao BID.

Além da seção 8 da licença acima, qualquer mediação relacionada a disputas decorrentes de tal licença deve ser conduzida de acordo com as Regras de Mediação da OMPI. Qualquer controvérsia relacionada ao uso das obras do BID que não possa ser resolvida amigavelmente deverá ser submetida à arbitragem de acordo com as regras da Comissão das Nações Unidas sobre Direito Comercial Internacional (UNCITRAL). O uso do nome do BID para qualquer outra finalidade que não a atribuição, bem como a utilização do logotipo do BID, serão objetos de um contrato por escrito de licença separado entre o BID e o usuário e não estão autorizados como parte desta licença.

Note-se que o link da URL inclui termos e condições que são parte integrante desta licença.

As opiniões expressas nesta publicação são de responsabilidade dos autores e não refletem necessariamente a posição do Banco Interamericano de Desenvolvimento, de sua Diretoria Executiva, ou dos países que eles representam.

Índice

Lista de tabelas e figuras Página 8

Agradecimentos Página 9

Siglas Página 10

Prefácio Página 11

Sumário executivo Página 14

1 Introdução

Quadro conceitual • Página 17

O que são ameaças cibernéticas? • Página 17

O que é um ciberataque? • Página 18

Definição de infraestrutura crítica • Página 19

A ascensão dos sistemas de TO • Página 20

Relação entre TO, ICS e SCADA • Página 21

A importância de proteger os ICS • Página 22

Tipos de ciberataques • Página 23

Atores de ameaças • Página 24

2 Proteção do setor de água e saneamento na era cibernética

A importância de proteger a infraestrutura crítica • Página 27

Previsões sobre a cibersegurança de IC como premissas para o planejamento estratégico • Página 27

Interdependências e segurança das infraestruturas • Página 28

Exemplos de interdependências de infraestrutura • Página 29

Interdependências entre água e águas residuais • Página 30

Cibersegurança no setor de água e saneamento • Página 31

Indústria 4.0 e o paradoxo da hiperconectividade • Página 31

Por que a Indústria 4.0 é importante para o setor de A&S? • Página 32

O impacto dos ciberataques na infraestrutura hídrica • Página 34

A tríade CIA sobre segurança de dados • Página 34

Elementos fundamentais que podem melhorar a postura de segurança cibernética do setor • Página 35

Danos potenciais e seu impacto na infraestrutura hídrica • Página 38

3 Preparação do setor de água e saneamento na América Latina e no Caribe

Cibersegurança regional na ALC • Página 41

Tendências regionais • Página 41

Proteção de infraestrutura crítica na região • Página 42

Por que a ALC é mais vulnerável a ciberataques?• Página 46

Por que não há mais ciberataques aos serviços públicos de água na ALC? • Página 47

Cooperação regional em matéria de cibersegurança • Página 47

Falta de incentivos • Página 48

Entrevistas: metodologia e perspectivas • Página 50

Cibersegurança no setor de água e saneamento na ALC • Página 51

Medidas específicas por país • Página 53

- Argentina • Página 53
- Brasil • Página 54
- Chile • Página 54
- Colômbia • Página 54
- República Dominicana • Página 54

4 Desafios e respostas em nível internacional

Entendendo a importância das parcerias público-privadas • Página 56

Estudos de casos internacionais • Página 57

Estudo de caso 1: o modelo israelense • Página 57

Estudo de caso 2: o modelo do Reino Unido • Página 59

5 Principais recomendações para o setor de água e saneamento da América Latina e Caribe

Principais recomendações de cibersegurança • Página 62

Questionário de autoavaliação para avaliar o cenário de cibersegurança em uma infraestrutura • Página 67

Bibliografia
Página 68

Apêndice A – Questionário de entrevista para empresas de serviços públicos
Página 76

Apêndice B – Questionário de entrevista para reguladores e órgãos federais
Página 78

Lista de tabelas e figuras

Tabela 1: Lista de atores de ameaças • Página 24

Tabela 2: Por que a indústria 4.0 é importante para o setor de A&S • Página 32

Tabela 3: Cenários de danos potenciais • Página 39

Tabela 4: Maturidade CMM do país na proteção de IC para a ALC • Página 44

Figura 1: Relação entre TO, ICS e SCADA • Página 21

Figura 2: Tipos de ciberataques • Página 23

Figura 3: Modelo de interdependências da infraestrutura • Página 29

Figura 4: Dependências de infraestrutura • Página 30

Figura 5: Etapas do tratamento da água • Página 33

Figura 6: Cinco estágios de maturidade • Página 43

Figura 7: Iniciativas de política de cibersegurança na ALC 1999–2019 • Página 49

Figura 8: Prioridades na estratégia de cibersegurança de Belize 2020-2030 • Página 50

Figura 9: Estratégia nacional de cibersegurança do Reino Unido • Página 60

Agradecimentos

Esta publicação faz parte da agenda de conhecimento desenvolvida pela Source of Innovation, uma parceria promovida e cofinanciada pela Divisão de Água e Saneamento (INE/WSA) do Banco Interamericano de Desenvolvimento (BID) e pelo BID Lab, em coordenação com parceiros importantes, como o governo da Suíça, por meio da Secretaria de Estado de Assuntos Econômicos (SECO), a Fundação FEMSA, o governo da Coreia, por meio do Ministério do Meio Ambiente, e o governo de Israel. Em colaboração com essa parceria, o estudo também foi codesenvolvido com a ajuda da equipe de segurança cibernética da Divisão de Inovação em Serviços ao Cidadão (IFD/ICS) do BID.

O produto de conhecimento gerado procura mostrar aos leitores as tendências, os desafios e as oportunidades da cibersegurança, no setor de água e saneamento da América Latina e do Caribe (ALC), avaliando a prontidão da cibersegurança da infraestrutura de água e esgoto da ALC e apresentando as principais recomendações para que os atores dos setores público e privado ampliem a resiliência cibernética geral de suas organizações.

Os autores agradecem a todas as pessoas que participaram da revisão e do aperfeiçoamento deste documento, em especial aos revisores María Donoso, James Pichardo e Iván Rodríguez. Agradecimentos especiais também são feitos a Ricardo Poppi, Kim Olson e Clara Sarcone por suas contribuições e trabalho louvável na revisão e edição do texto. Por último, mas não menos importante, o BID também agradece às organizações e aos profissionais que gentilmente concordaram em participar de nossas entrevistas e consultas, fornecendo informações valiosas necessárias para a conclusão desta publicação.

Siglas

APT: Ameaça persistente avançada

A tríade CIA: O modelo de confidencialidade, integridade e disponibilidade

ALC: América Latina e Caribe

A&S: Água e saneamento

BID: Banco Interamericano de Desenvolvimento

CERT.br: Equipe de resposta a emergências informáticas do Brasil

CLP: Controle lógico programável

CMM: Modelo de maturidade de capacidade de cibersegurança para nações

CSO: Transbordamentos de esgoto combinado

IC: Infraestrutura crítica

ICS: Sistemas de controle industrial

IIoT: Internet industrial das coisas

IoT: Internet das coisas

NCSC: Centro Nacional de Segurança Cibernética do Reino Unido

NCSS: Estratégia Nacional de Cibersegurança

NIST: Instituto Nacional de Padrões e Tecnologia dos Estados Unidos

OEA: Organização dos Estados Americanos

PPP: Parcerias público-privadas

SCADA: Controle de supervisão e aquisição de dados

SSO: Transbordamentos de esgoto sanitário

TI: Tecnologia da informação

TIC: Tecnologia de informação e comunicação

TO: Tecnologia operacional

Prefácio

A digitalização é um elemento fundamental para a governança do século XXI, ajudando os Estados a melhorar a qualidade e a cobertura dos serviços públicos que prestam, bem como a aumentar a integridade de suas atividades em benefício da sociedade.

Embora a pandemia da COVID-19 tenha servido como um acelerador recente para a digitalização, os setores público e privado começaram o século XXI com esforços significativos de investimento em infraestrutura tecnológica, sistemas digitais e talentos humanos, buscando melhorar sua gestão e seus serviços. Os cidadãos puderam acessar mais serviços e informações com facilidade e eficiência, usando canais inovadores de comunicação com governos e empresas.

Conscientes de que a digitalização é uma ferramenta que promove eficiência, agilidade e transparência na operação do setor público, e que também contribui para melhorar a qualidade de vida da população da América Latina e do Caribe, o Banco Interamericano de Desenvolvimento promove a implementação de tecnologias digitais nos países da região.

Com as oportunidades descritas, esse processo de digitalização traz consigo complexidades e desafios. À medida que a digitalização de infraestruturas e serviços urbanos aumenta, também aumenta sua exposição aos riscos e vulnerabilidades inerentes ao espaço cibernético, abrindo a porta para atores mal-intencionados e ciberataques que buscam prejudicar áreas críticas como água e saneamento (A&S) (Guillaume, 2022), saúde, energia, transporte, entre muitas outras.

Nesse contexto de infraestrutura crítica, os sistemas digitalizados de A&S são classificados como um dos mais sensíveis (IWA, 2022), devido à sua relação intrínseca com a saúde da população e os controles de higiene, englobando responsabilidades como a produção e o fornecimento contínuo de água potável para os cidadãos, juntamente com a coleta, o transporte e o tratamento de águas residuais, entre outros processos fundamentais para as condições sanitárias de áreas residenciais e públicas. Dada a criticidade dessas operações, não é de surpreender que um relatório da American Water Works Association tenha apontado o risco cibernético como a principal ameaça enfrentada pelo setor de A&S (Germano, 2019).

Um ciberataque direcionado às dependências do setor de A&S tem a capacidade de prejudicar, ou até mesmo interromper, as operações de cidades inteiras, causando danos significativos e, em certos casos, irreparáveis ou catastróficos aos sistemas de tecnologia do Estado, deixando a população sem abastecimento de água por períodos de várias horas, ou até mesmo dias, e aumentando a possibilidade de se contrair doenças associadas à ingestão de água não tratada ou contaminada, e, consequentemente, colocando em risco a vida das pessoas.

Ao mesmo tempo, certas práticas tradicionais de infraestruturas digitalizadas, como monitoramento, coleta de dados e manutenção extensiva de registros, podem ser exploradas por criminosos cibernéticos que buscam obter informações confidenciais dessas instalações de tratamento de água para fins ilícitos, como divulgar dados de clientes e fornecedores, encontrar vulnerabilidades no órgão de gestão da empresa ou do Estado, interromper a cadeia de suprimentos ou até mesmo vender as informações para concorrentes no mercado clandestino.

Os motivos pelos quais a infraestrutura de A&S enfrenta esses tipos de ameaças diariamente são tão variados quanto os métodos de ataque usados pelos criminosos cibernéticos. Interesses pessoais, políticos e econômicos, entre outros, levam os criminosos a desenvolver novas ferramentas e métodos, estudando esses sistemas e encontrando vulnerabilidades que, com o tempo, lhes permitirão aumentar a frequência e a sofisticação desses incidentes.

Para combater essas ameaças, é responsabilidade das administrações planejar e investir proativamente para garantir que os ciberataques não causem interrupções em sua gestão e coloquem em risco a população. O investimento em cibersegurança é o principal mecanismo para cumprir esse objetivo de defender e apoiar a digitalização dessas entidades críticas para a saúde de seus usuários e dos serviços digitais que possuem.

Este estudo tem como objetivo fornecer uma visão geral da proteção cibernética que os países da região implementam em suas entidades de coleta, tratamento e distribuição de água operadas em seu território nacional. Fornece informações compiladas de várias fontes, especialistas e publicações, com base nas quais é apresentada uma análise abrangente do nível de preparação do setor, com ênfase na importância de proteger essas infraestruturas críticas no ambiente da Quarta Revolução Industrial (Stankovic, Hasanbeigi e Neftenov, 2020).

Trazendo argumentos como o custo do crime cibernético, as tendências na região, os principais incentivos e desafios em nível internacional, entre outros, baseia-se na experiência de países com políticas reconhecidas de cibersegurança, como Israel e Reino Unido, para apresentar estudos de caso que detalham os resultados de uma gestão sólida e comprometida com a segurança da informação no setor. Com base na análise de todas essas experiências e recomendações, o estudo é proposto como uma ferramenta para promover o conhecimento e as principais ações de defesa cibernética para garantir o futuro do setor de A&S.

No BID, estamos cientes desses desafios e, por isso, estamos trabalhando em estreita colaboração com os fornecedores de A&S e os governos da região, apoiando a digitalização segura que fortalece seus recursos de cibersegurança. A implementação de políticas abrangentes de cibersegurança possibilitará o aproveitamento dos benefícios da Quarta Revolução Industrial, garantindo o bem-estar da população. Convidamos você a se juntar a nós nesse esforço.

Roberto de Michele
Chefe da Divisão de Inovação em Serviços ao Cidadão
Setor de Instituições para o Desenvolvimento
Banco Interamericano de Desenvolvimento

Sergio Campos
Chefe da Divisão de Água e Saneamento
Setor de Infraestrutura e Energia
Banco Interamericano de Desenvolvimento

Sumário executivo

O setor de água e saneamento é essencial para sobrevivência e, portanto, tem sido considerado pela maioria dos países como infraestrutura crítica (WHO, 2019). Embora a tendência crescente de automação e digitalização das instalações do setor de A&S melhore a eficiência e ajude a reduzir os custos operacionais, ela também expõe as instalações e operações do setor a riscos cibernéticos cada vez maiores. O número e a variedade de ameaças cibernéticas e atores maliciosos que visam os serviços públicos tem aumentado rapidamente: desde atores de estados-nações que procuram causar caos político e social, e também perturbar as economias, cibercriminosos à procura de lucro, *hacktivistas* motivados por agendas ideológicas ou pessoais e *insiders* descontentes até indivíduos que tentam obter um alívio nas suas contas.

À medida que as tecnologias digitais se espalham e agregam maior valor à infraestrutura hídrica, os cibercriminosos tentam explorar a infraestrutura interconectada atacando os sistemas de controle industrial (ICS), os computadores especializados que gerenciam operações de fluxo, tratamento de águas residuais e muito mais. Os ciberataques vão aumentar em frequência, volume e sofisticação. No entanto, a consciência limitada, associada à relutância em investir em cibersegurança devido a seus custos, além da falta de atenção e de requisitos regulamentares, resultará em subinvestimento das concessionárias em cibersegurança e vulnerabilidade elevada a ciberataques – um resultado que pode ter consequências severas.

As concessionárias de água em todo o mundo já enfrentaram uma ampla gama de ataques, desde *ransomware* e adulteração de ICS até a manipulação de operações de válvulas e fluxo, afetando formulações de tratamento químico, além de outras tentativas de danificar máquinas e interromper as operações. Entrevistas realizadas durante este estudo revelaram que algumas entidades da ALC já sofreram um evento cibernético que afetou suas operações, embora a recuperação tenha acontecido rapidamente. No entanto, a própria capacidade de uma entidade de classificar um evento operacional como um incidente cibernético depende muito de sua infraestrutura digital, capacidades de investigação criminalística e consciência cibernética.

Os ciberataques direcionados aos sistemas do setor de A&S podem comprometer o fornecimento de água potável, a qualidade da água ou a coleta e tratamento de águas residuais, interrompendo a continuidade e a confiabilidade dos negócios ou processos. Esses ataques também podem manipular informações de consumo, interferir no faturamento e comprometer os dados dos clientes. Os ciberataques a entidades que gerenciam água ou águas residuais podem ter efeitos devastadores na saúde pública, no meio ambiente e na economia. Além disso, os ciberataques que resultam em contaminação, mau funcionamento operacional ou interrupções de serviço podem, em última análise, minar a confiança do cliente e até resultar em responsabilização financeira e legal.

Este documento é o primeiro de seu tipo publicado pelo Banco Interamericano de Desenvolvimento para examinar as ameaças cibernéticas no setor de A&S da ALC, que são motivo de crescente preocupação. O BID, em parceria com a Organização dos Estados Americanos (OEA), realizou estudos abrangentes para avaliar a maturidade cibernética de cada país da ALC em 2020, usando o Modelo de Maturidade da Capacidade de Cibersegurança para as Nações, conhecido como modelo CMM. O BID publica guias de cibersegurança de interesse geral, bem como guias de melhores práticas de cibersegurança para outros setores críticos, como eletricidade, saúde e cidades inteligentes. Este documento vem ampliar os conhecimentos mais recentes disponíveis no setor de A&S da ALC, disponibilizados publicamente pelo BID, abordando questões abrangentes, entre elas, a transformação digital do setor.

Este relatório analisa as tecnologias do setor de A&S e explica as ameaças cibernéticas enfrentadas pela tecnologia de infraestrutura hídrica. Avalia a prontidão de cibersegurança do setor de A&S da ALC usando material escrito e entrevistas com importantes representantes de instituições do setor público e outras concessionárias de água na ALC. Por último, são apresentadas uma série de recomendações para os intervenientes dos setores público e privado. Além disso, um questionário de autoavaliação on-line gratuito foi implementado para permitir que as organizações avaliem sua postura atual de cibersegurança, identificando as lacunas existentes e fornecendo recomendações.

A cibersegurança efetiva no setor de A&S requer não apenas a implementação de medidas técnicas e metodologias, mas sua priorização e integração na gestão e na cultura corporativas. Isso fortaleceria a cibersegurança do setor, permitindo o fornecimento seguro e ininterrupto de serviços essenciais de água e saneamento para as pessoas na ALC.

KT Stock photos / shutterstock.com

1

Introdução

Quadro conceitual

O que são ameaças cibernéticas?

O rápido e contínuo desenvolvimento da tecnologia, aliado à nossa crescente dependência dela, representou uma ameaça emergente nos últimos anos, afetando todas as áreas da vida: a ameaça cibernética. Hoje, muitos processos críticos para o nosso bem-estar são controlados e apoiados por sistemas de tecnologia da informação, como os sistemas de água e eletricidade, telecomunicações e serviços de transporte. Essa nova ameaça desafia governos, empresas, organizações e cidadãos em todo o mundo.

Esses processos e a ameaça emergente ocorrem em um domínio conhecido como ciberespaço. De acordo com o Centro de Pesquisa em Segurança da Computação (CSRC) do Instituto Nacional de Padrões e Tecnologia (NIST) dos EUA, o ciberespaço pode ser descrito como a rede interdependente de infraestruturas de tecnologia da informação, incluindo a internet, redes de telecomunicações, sistemas de computadores e processadores e controladores incorporados em indústrias críticas (CSRC, 2022a).

O que é um ciberataque?

O CSRC (2022b) define ciberataque como um ataque, via ciberespaço, que visa o uso do ciberespaço por uma empresa com a finalidade de interromper, desativar, destruir ou controlar maliciosamente um ambiente ou infraestrutura de computação, destruindo a integridade dos dados ou roubando informações controladas.

Alguns ciberataques são realizados explorando vulnerabilidades em plataformas tecnológicas. Uma vulnerabilidade de cibersegurança é uma fraqueza tecnológica ou um comportamento não intencional em um sistema de computador que permite que potenciais invasores tenham acesso a ele ou executem ações que não deveriam ser permitidas. As vulnerabilidades permitem vários níveis de acesso não autorizado a um sistema de informação, que os invasores podem usar para realizar uma série de ações, dependendo de seus objetivos e intenções. Há uma distinção entre vulnerabilidades que foram expostas e para as quais os desenvolvedores de software lançaram uma atualização de segurança que as impede de serem exploradas, as "vulnerabilidades conhecidas", e as vulnerabilidades que foram expostas pelos pesquisadores, mas não têm nenhuma atualização de segurança para impedir que sejam exploradas, as chamadas vulnerabilidades "de dia zero" ("Zero-Day"). Diante disso, os programadores de software não têm tempo suficiente para desenvolver uma atualização de segurança antes que a vulnerabilidade possa ser explorada para fins maliciosos (Ablon e Bogart, 2017).

Bayazed / Shutterstock.com

Definição de infraestrutura crítica

Em escala nacional, a infraestrutura é caracterizada como crítica quando se acredita que seu fracasso causará uma crise socioeconômica considerável, com potencial de desestabilizar a sociedade e com ramificações políticas, estratégicas ou de segurança. Diferentes países definem infraestrutura crítica (IC) de forma diferente, mas o que todos têm em comum, em nosso contexto, é que se trata de uma infraestrutura com uma dimensão informatizada, da qual outros sistemas físicos dependem e cuja falha de funcionamento pode causar danos consideráveis à dimensão física (Tabansky, 2011). Para a infraestrutura hídrica, esse dano pode se estender além do sistema sociopolítico para afetar estruturas físicas reais (barragens, sistemas de distribuição, etc.) e o meio ambiente.

Em alguns países, a definição de IC baseia-se na designação formal da infraestrutura, enquanto em outros, é baseada nas consequências sociais dos danos causados a ela. Por exemplo, a União Europeia define IC como sistemas necessários para a segurança nacional e transfronteiriça de serviços essenciais pertencentes a setores como TIC, energia, finanças, saúde e transportes (ENISA, 2023). Nos Estados Unidos, o termo infraestrutura crítica refere-se a sistemas, ativos ou redes (físicas ou virtuais) que são de importância crucial, pois sua destruição teria sérias consequências para a segurança nacional, em geral, e para a segurança econômica, em particular, e também para a saúde pública (CISA, 2023). Visto que os países definem a IC de maneira diferente, os setores onde essa infraestrutura pode ser encontrada também variam. De acordo com a Agência de Cibersegurança e Segurança de Infraestrutura dos EUA (CISA), sistemas críticos de infraestrutura podem ser encontrados, entre outros, nos setores de energia, de alimentos e agricultura, de comunicações, nos sistemas de transporte e no setor de sistemas de água e águas residuais (CISA, 2022).

Muitos sistemas de IC são gerenciados e operados por meio de sistemas digitais de controle e monitoramento conhecidos como Controle de Supervisão e Aquisição de Dados (SCADA), que fazem a mediação entre o mundo físico e o ciberespaço por meio de Controladores Lógicos Programáveis (CLP). Os sistemas SCADA permitem o acesso remoto em alguns casos. Quanto aos sistemas de água, muitas vezes, é possível controlar remotamente a operação e o desligamento de bombas que retiram água dos reservatórios, dependendo das necessidades e da quantidade de água no reservatório, além de controlar o fluxo de água nas barragens e, se necessário, o seu fechamento (Keith Stouffer *et al.*, 2015).

American Public Power Association/ Shutterstock.com

A ascensão dos sistemas de TO

O hardware e o software utilizados com os sistemas de controle de automação dentro da infraestrutura são chamados de Tecnologia Operacional (TO) (Murray, Johnstone e Valli, 2017). Os sistemas de TO são usados em todo o mundo para controlar e monitorar processos industriais em instalações e IC, como usinas de energia, usinas nucleares e infraestrutura de água e esgoto.

Na última década, a ascensão da Internet Industrial das Coisas (IIoT) resultou na convergência da Tecnologia da Informação (TI) e da TO. As indústrias conectaram sistemas de TI e TO em um esforço para melhorar a funcionalidade da infraestrutura, eliminando assim as chamadas lacunas de ar que protegiam seus sistemas de TO de *hackers* e *malware* originários da internet mais ampla. Facilitados pela eliminação da lacuna de ar, os atores hostis aumentaram seus esforços de *hacking* contra sistemas de TO para obter dados, interromper operações ou lançar ciberataques terroristas contra a IC (Siboni, Cohen e Rotbart, 2013). Esses riscos estão aumentando com o número cada vez maior de dispositivos conectados, muitos dos quais não são protegidos por seus fabricantes ou usuários, e também com o aumento na ocorrência de ataques de interrupção de serviço em sistemas públicos e privados, com demandas de extorsão e pagamento de resgate (Siboni, Cohen e Rotbart, 2013). Os *malware* existentes são eficazes contra sistemas desatualizados instalados em redes de TO que sofrem de falta de controles de cibersegurança e falta de proteção cibernética adicional, como proteção de cibersegurança de *endpoint* (software antivírus) (Stouffer *et al.*, 2015).

Os ataques contra sistemas que controlam e monitoram infraestruturas civis críticas são classificados no topo da escala de gravidade dos ciberataques. Entre os mais graves estão ataques que colocam em risco vidas civis, incluindo poluição da água ou danos ambientais, devido a derramamentos de esgoto ou de produtos químicos, também conhecidos como transbordamentos de esgoto sanitário (SSO). Nos últimos anos, também houve aumento significativo nos ciberataques à IC de diversos atores, incluindo estados, terroristas, anarquistas, entidades comerciais concorrentes, criminosos, integrantes da organização que agem de forma maliciosa ou inadvertida e outros (Bigelow e Lutkevich, 2021). Os ataques a organizações em setores críticos de infraestrutura aumentaram drasticamente, de menos de 10, em 2013, para quase 400, em 2020 – uma mudança de 3.900% (Thielemann *et al.*, 2021).

Muitas organizações tradicionalmente consideram a TO, que lida com máquinas e o mundo físico, como segura contra ciberataques. As organizações com frequência se esforçam muito para fortalecer seu perímetro, mas inadequadamente orçam e investem em segurança interna, com ênfase na segurança do sistema de TO. Essas discrepâncias de investimento deixam a TO menos protegida e aberta a ataques. Uma vez que os invasores tenham obtido acesso aos sistemas de uma organização, podem facilmente se movimentar e atuar dentro deles. Dois ciberataques em 2017 (NotPetya e WannaCry) demonstraram na prática que trabalhar de acordo com esse modelo tradicional não é mais suficiente (Bigelow e Lutkevich, 2021).

Relação entre TO, ICS e SCADA

É importante diferenciar entre os papéis de TO, ICS e SCADA. TO refere-se a sistemas de computação usados para gerenciar operações industriais. O SCADA é usado para exibir dados, e ICS, os sistemas que monitoram, controlam e gerenciam processos industriais ou de automação, é o nível entre TO e SCADA. A maioria dos ICS são considerados sistemas de controle de processo contínuo gerenciados por CLP ou sistemas de controle de processo discretos (DPC) que podem usar um CLP ou algum outro dispositivo de controle de processo em lote. Essencialmente, a TO diz ao sistema "o que fazer", o ICS verifica o resultado dos sistemas ("como você fez?") e o SCADA processa os dados coletados no ICS e os torna acessíveis aos usuários (Williamson, 2015). A Figura 1 abaixo ilustra isso.

Figura 1: Relação entre TO, ICS e SCADA

Fonte: Williamson (2015).

A importância de proteger os ICS

Os ICS são cruciais para as organizações industriais, pois auxiliam na manutenção da eficiência, avaliam os dados, para que escolhas informadas possam ser feitas, e identificam falhas nos sistemas para ajudar a garantir a qualidade e diminuir o tempo de inatividade (Stouffer *et al.*, 2015). Eles podem ser encontrados em todas as instalações operacionais e em uma variedade de outras entidades, mas, apesar de sua onipresença, muitos permanecem vulneráveis a ciberataques.

Muitos protocolos de comunicação usados nos ICS têm décadas e não foram projetados para lidar com os riscos cibernéticos atuais. Alguns dispositivos, protocolos e programas dos ICS, por exemplo, podem ser modificados sem autenticar o usuário, e alguns são expostos à internet. Além disso, os ICS foram construídos para serem totalmente independentes de qualquer outro sistema por razões de confiabilidade. No entanto, considerações de custo e eficiência levam os operadores para conectar os ICS às redes industriais e até mesmo à internet, mesmo que não tenham sido destinados a esse ambiente, colocando-os em maior risco de ciberataques, uma vez que ficam expostos ao mundo exterior, sem a segurança adequada (Stouffer *et al.*, 2015).

De acordo com o relatório semestral de risco e fraqueza publicado por uma empresa de segurança cibernética que trabalha no domínio dos ICS, a conscientização sobre o campo de segurança desses sistemas aumentou devido a ciberataques de alto nível em IC e instalações industriais. Consequentemente, houve aumento drástico na detecção de vulnerabilidades de segurança nos ICS, assim como o aumento da conscientização pública e governamental sobre a segurança desses sistemas. Das 637 vulnerabilidades de ICS que afetam 76 fornecedores, publicadas pela Claroty, no primeiro semestre de 2021, 65% têm alta probabilidade de causar uma perda total de disponibilidade no sistema (Claroty Team82, 2021).

Stouffer *et al.* (2015) relatam as duas dinâmicas de ataque mais comuns contra ICS como:

1. Ataques destinados a interromper uma função operacional, causando danos imediatos.

2. Ataques lentos e secretos que se baseiam em mudanças lógicas nos sistemas de controle e/ou na compreensão profunda do processo para manipulá-lo deliberadamente.

Tipos de ciberataques

No ciberespaço, o fator humano é responsável pela maioria das falhas e do mau funcionamento. Em 2017, aproximadamente 52% dos empresários dos Estados Unidos reconheceram o risco de um ciberataque devido ao fator humano, resultante de ato ou omissão por parte dos funcionários de uma organização (Kaspersky, 2017b). A Figura 2 abaixo fornece uma breve descrição de vários tipos de ciberataques.

Figura 2: Tipos de ciberataques

Fonte: autores – adaptado de Check Point Software (s.d.).

Atores de ameaças

O Canadian Centre for Cyber Security (2018) relata que vários atores de ameaças podem ter interesse em interromper a função adequada da infraestrutura hídrica em função de interesses ideológicos, econômicos, políticos, pessoais ou outros. A Tabela 1 abaixo lista os principais tipos de atores de ameaça.

Tabela 1: Lista de atores de ameaças

Atores de estado-nação

Os estados soberanos atacam vários alvos no ciberespaço, causando efeitos variados, desde a desfiguração de websites até danos extensos à infraestrutura. Seu objetivo é geralmente geopolítico.

Cibercriminosos
(Atores de ameaças motivados financeiramente)

Um dos motivos mais comuns para os cibercriminosos é o lucro. Eles tendem a visar organizações pouco protegidas, que são vulneráveis a interrupções e têm capacidade de pagamento, ou cujos ativos valiosos, como dados, propriedade intelectual ou fundos, podem ser roubados on-line.

Atacantes patrocinados por Estados e grupos de ameaça persistente avançada (APT)

Os grupos de APTs são atores de ameaças muito capazes tecnicamente. Alguns APTs são patrocinados por Estados, mas mantêm uma negação plausível, pois em geral não fazem parte abertamente de um governo. Os grupos de APTs perseguem os objetivos estratégicos dos países e podem usar recursos avançados de maneira sustentada para atacar entidades grandes e possivelmente melhor protegidas. Seus alvos podem incluir instituições estatais, IC e empresas que possuem bens essenciais. A meta comum desses invasores é alcançar um objetivo estratégico para seu patrocinador, na forma de disrupção ou obtenção de informações confidenciais. Exemplos recentes incluem o ciberataque à SolarWinds, que explorou vulnerabilidades na cadeia de fornecimento de software.

Terroristas

Estes atores estão interessados em concretizar sua ideologia usando a violência contra a população civil. Os terroristas, às vezes, usam abordagens pouco sofisticadas, aplicando ferramentas amplamente disponíveis, que exigem poucas habilidades técnicas para serem implantadas.

Atores de ameaças internas

Quaisquer funcionários, fornecedores ou prestadores de serviço atuais ou antigos de uma organização, que tenham acesso legítimo a seus sistemas e instalações, podem representar uma ameaça cibernética potencial. Esses indivíduos podem ter amplo conhecimento dos sistemas e controles de segurança da organização. Aqueles que decidem usar seus conhecimentos contra sua organização geralmente são movidos por vingança (categorizados como funcionários descontentes), razões psicológicas, ideológicas ou financeiras. Eles normalmente querem prejudicar a reputação da organização ou roubar informações confidenciais, como propriedade intelectual.

Hacktivistas

Indivíduos ou grupos como o Anonymous que usam *hacking* para promover seus objetivos sociais ou ideológicos. Na maioria dos casos, seu principal objetivo é aumentar a conscientização sobre a causa, em vez de causar especificamente danos à IC.

Fonte: autores – adaptado de Flashpoint (2021).

Na ALC, as ameaças proeminentes geralmente são motivadas financeiramente, como ataques por FIN11 e UNC2053 (dois grupos de crimes financeiros bem estabelecidos) e, muitas vezes, assumem a forma de ataques de *ransomware* e *malware*. De acordo com a Mandiant, os anúncios de dados roubados de organizações da ALC durante incidentes de *ransomware* aumentaram 550% em apenas um ano (de 2020 a 2021). Essa atividade afetou vários países, com maior frequência o Brasil, a Colômbia e o México, e envolveu instalações industriais, incluindo fornecedores de energia e outras concessionárias (Caparros, 2022).

Marlo Wock / Unsplash.com

Proteção do setor de água e saneamento na era cibernética

A importância de proteger a infraestrutura crítica

Conforme descrito na introdução, a IC é definida como tal pelo impacto de sua falha, o que poderia desencadear uma crise considerável. É importante planejar e implementar proteções de IC de maneira estratégica, considerando uma série de previsões que descrevemos mais detalhadamente nesta seção.

Previsões sobre a cibersegurança de IC como premissas para o planejamento estratégico

Embora os seguintes prognósticos possam não se aplicar totalmente à ALC, eles fornecem um ponto de partida geral para o planejamento estratégico.

Até 2024, um ciberataque irá danificar IC, de forma que um membro do G20 retribuirá com um ataque físico declarado. Além disso, 80% das organizações de IC abandonarão seus provedores de soluções de segurança em silos existentes, a fim de superar os riscos ciberfísicos e de TI, adotando soluções hiperconvergentes (Snow, 2022).

Até 2025, os invasores terão transformado em arma um sistema ciberfísico de IC para prejudicar ou matar humanos intencionalmente e com sucesso (Moore, 2021a).

Em 2025, 30% das organizações de IC sofrerão uma violação de segurança que resultará na interrupção das operações ou de um sistema ciberfísico de missão crítica (Moore, 2021b).

Em 2026, menos de 30% dos proprietários e operadores de IC dos Estados Unidos atenderão aos requisitos de segurança do governo recentemente exigidos para sistemas ciberfísicos (Snow, 2022).

Interdependências e segurança das infraestruturas

O crescente uso de TI, aliado à crescente dependência do livre mercado de produtos e serviços fornecidos como infraestrutura, aumenta a prevalência da interdependência da infraestrutura e a importância do fenômeno pelo qual os danos causados a um sistema de infraestrutura afetam outro. A interrupção de um sistema de infraestrutura pode ter impacto significativo na capacidade de outras infraestruturas operarem e, em muitos casos, pode resultar no colapso de outras infraestruturas conectadas àquela afetada (Menashri e Baram, 2015). É por isso que a IC dos Estados Unidos é frequentemente chamada de um "sistema de sistemas" (Stouffer *et al.*, 2015).

A capacidade de identificar e analisar interdependências é claramente uma parte importante da proteção da IC. Embora as interdependências sejam uma característica comum dos sistemas de IC e, muitas vezes, se materializem por conexões digitais por meio da tecnologia da informação e comunicação, a maioria é determinada regionalmente, ou seja, está intimamente relacionada à proximidade geográfica e às redes regionais integradas. Isso é particularmente verdadeiro, por exemplo, na região do Mar Báltico, e especialmente nos países nórdicos, onde as IC de muitos setores fazem parte do mesmo sistema de infraestrutura nórdica (Pursiainen *et al.*, 2007).

Os atores envolvidos na proteção cibernética da infraestrutura devem estudar e examinar as conexões e dependências entre as várias infraestruturas, criar redundâncias e projetar sistemas para serem resilientes aos efeitos cascata (os chamados "efeitos dominó"), impactando outras infraestruturas altamente dependentes em caso de perda ou dano a uma delas (Menashri e Baram, 2015). Ao realizar avaliações de vulnerabilidade, estabelecer planos de resposta e recuperação e gerenciar outras preocupações de segurança e proteção, os sistemas de água e esgoto têm interdependências distintas com outras infraestruturas que devem ser consideradas (Gillette *et al.*, 2002).

Aleksei Zaitcev / Unsplash.com

Exemplos de interdependências de infraestrutura

De acordo com um modelo sugerido por Steven Rinaldi em um estudo realizado com outros pesquisadores (Rinaldi, Peerenboom e Kelly, 2001), quatro tipos de interdependências podem ser identificados:

Interdependência física: quando um sistema depende da saída física de outro(s) sistema(s).

Interdependência geográfica: quando o(s) sistema(s) pode(m) ser afetado(s) por uma mudança no ambiente próximo.

Interdependência cibernética: quando os sistemas estão se comunicando através do ciberespaço.

Interdependência lógica: quando os sistemas são dependentes uns dos outros em qualquer outra forma de interdependência, que não as especificadas acima.

O modelo incluído na Figura 3 apresenta uma imagem visual das interdependências descritas.

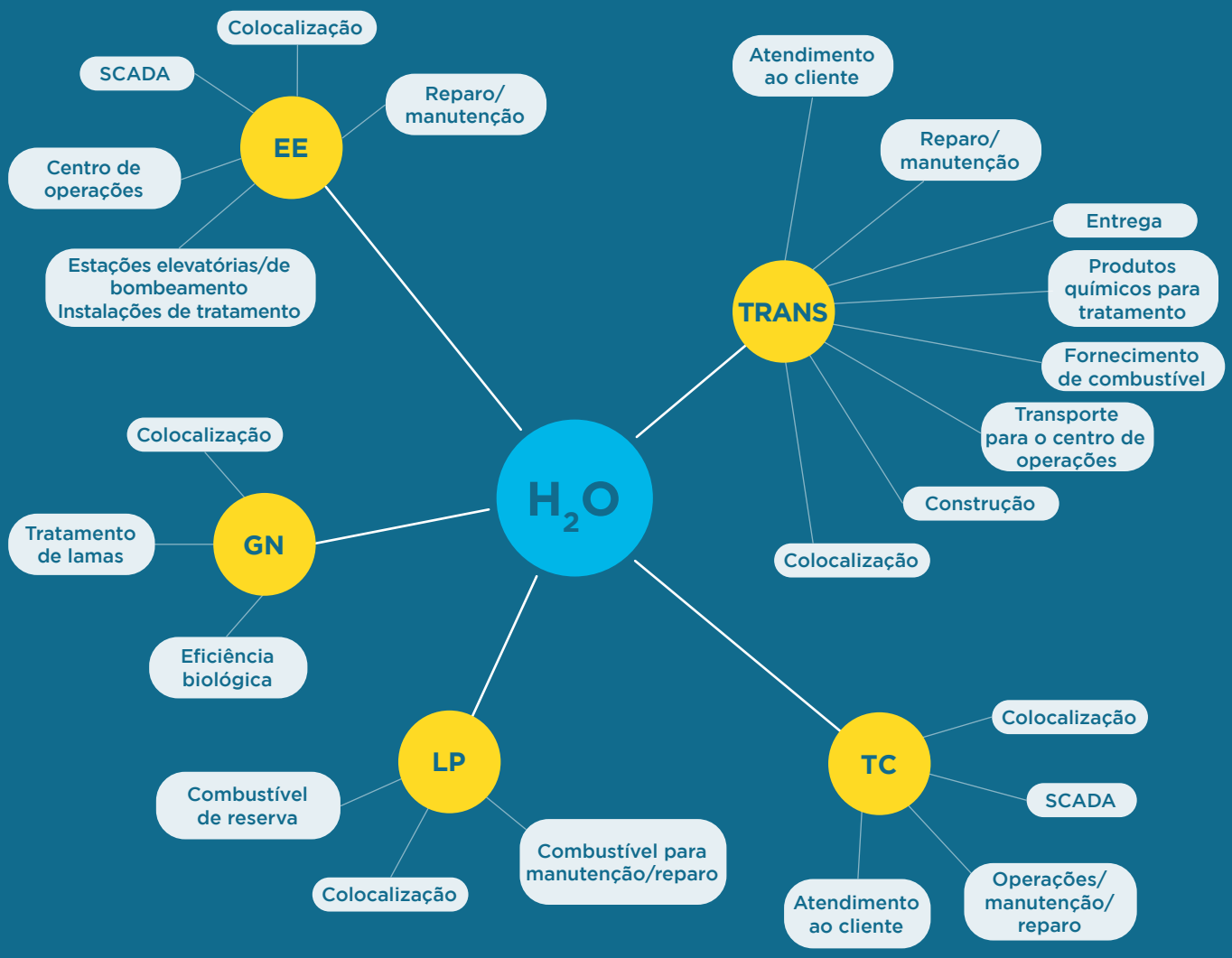
Figura 3: Modelo de interdependências da infraestrutura

Fonte: Rinaldi, Peerenboom e Kelly (2001).

Interdependências entre água e águas residuais

Ao estudar as vulnerabilidades cibernéticas e projetar suas respectivas proteções de cibersegurança, a interdependência específica da infraestrutura de águas residuais e água deve ser examinada, pois essas infraestruturas estão ligadas aos principais fornecedores de água potável de um país ou região (Gillette *et al.*, 2002). Como exemplo, podemos olhar para o terremoto de 2009 em Cinchona, na Costa Rica, que causou fortes deslizamentos de terra e fluxos de lama que resultaram em danos aos sistemas de água e esgoto e teve impactos significativos na disponibilidade de água potável. Mostra como os desastres naturais podem influenciar as instalações de águas residuais e, como resultado, afetar a disponibilidade de água potável (Deubelli, 2019). A Figura 4 ilustra as dependências de infraestrutura, incluindo suas dependências de outros tipos de infraestruturas (transporte, gás, etc.).

Figura 4: Dependências de infraestrutura



Notas: **H_2O - o setor de A&S, EE – energia elétrica, GN – gás natural, LP – líquidos de petróleo, TRANS – transporte, TC – telecomunicações.**

Fonte: Gillette *et al.* (2002).

Com base em entrevistas realizadas durante este estudo, descobrimos que, na maioria dos países, incluindo os da ALC, a infraestrutura de água e esgoto é antiga e não tão eficiente quanto pode ser. Portanto, a indústria deve passar por uma transformação digital para expandir e garantir o acesso contínuo à água potável. A digitalização está melhorando as operações de serviços públicos, aumentando sua eficiência, aperfeiçoando os serviços e atualizando suas tecnologias. Além de ampliar a cobertura de serviços para mais pessoas, a digitalização traz benefícios financeiros: empresas que possuem maior maturidade digital relatam crescimento de receita de 30% a mais em relação às empresas de menor maturidade (Deloitte Insights, 2020).

À medida que o setor de A&S se torna mais digitalizado, também se torna cada vez mais vulnerável a ciberataques. A falta de conscientização sobre os riscos cibernéticos, resultando na falta de investimentos para mitigá-los, aumenta seus danos potenciais. Conforme proposto por Mirjana *et al.* (2020), a cibersegurança no setor industrial, que depende de tecnologias de IIoT e é vulnerável a ciberataques especializados, deve ser gerenciada por meio de estruturas adequadas, o que fortalecerá a resiliência cibernética dessas infraestruturas.

Cibersegurança no setor de água e saneamento

Indústria 4.0 e o paradoxo da hiperconectividade

A Indústria 4.0 refere-se à quarta revolução industrial, na qual o setor industrial se torna mais digitalizado e automatizado e adota novas tecnologias em processos industriais, como IA, Big Data, *blockchain*, drones e realidade virtual e aumentada (VR/AR). O setor de A&S está se transformando em direção à visão da Indústria 4.0, que introduzirá desafios inteiramente novos devido à complexa hiperconectividade e ao aumento do leque de ameaças. A incorporação de dispositivos de IoT apresenta preocupações sobre perda de dados, roubo de informações, privacidade, proteção de rede enfraquecida e muito mais. À medida que dispositivos adicionais estão sendo conectados a redes operacionais, as concessionárias enfrentam maior vulnerabilidade, e os *hackers* têm mais oportunidades de acessar redes uma vez que usam vetores adicionais de ataque.

As soluções de medição remota (medição inteligente) são um exemplo claro da evolução do setor em direção à Indústria 4.0. A evolução das tecnologias de comunicação significa que os sistemas são operados remotamente e gerenciados centralmente. Graças à captura de dados mais frequente e de maior qualidade, as empresas podem oferecer serviços novos e aprimorados aos clientes, como comunicação proativa de problemas, aviso sobre consumo fora do normal de água e recomendações para consumo responsável. Além de melhorias qualitativas nos serviços diretos ao cidadão, a medição remota oferece a possibilidade de gestão aprimorada da rede inteligente, detecção precoce de vazamentos, melhor eficiência energética e, finalmente, otimização de processos e gestão integrada eficiente do ciclo da água (Mirjana *et al.*, 2020).

Por que a Indústria 4.0 é importante para o setor de A&S?

Mirjana *et al.* (2020) afirmam que no setor de A&S, a Indústria 4.0 é particularmente importante pelas razões destacadas na Tabela 2.

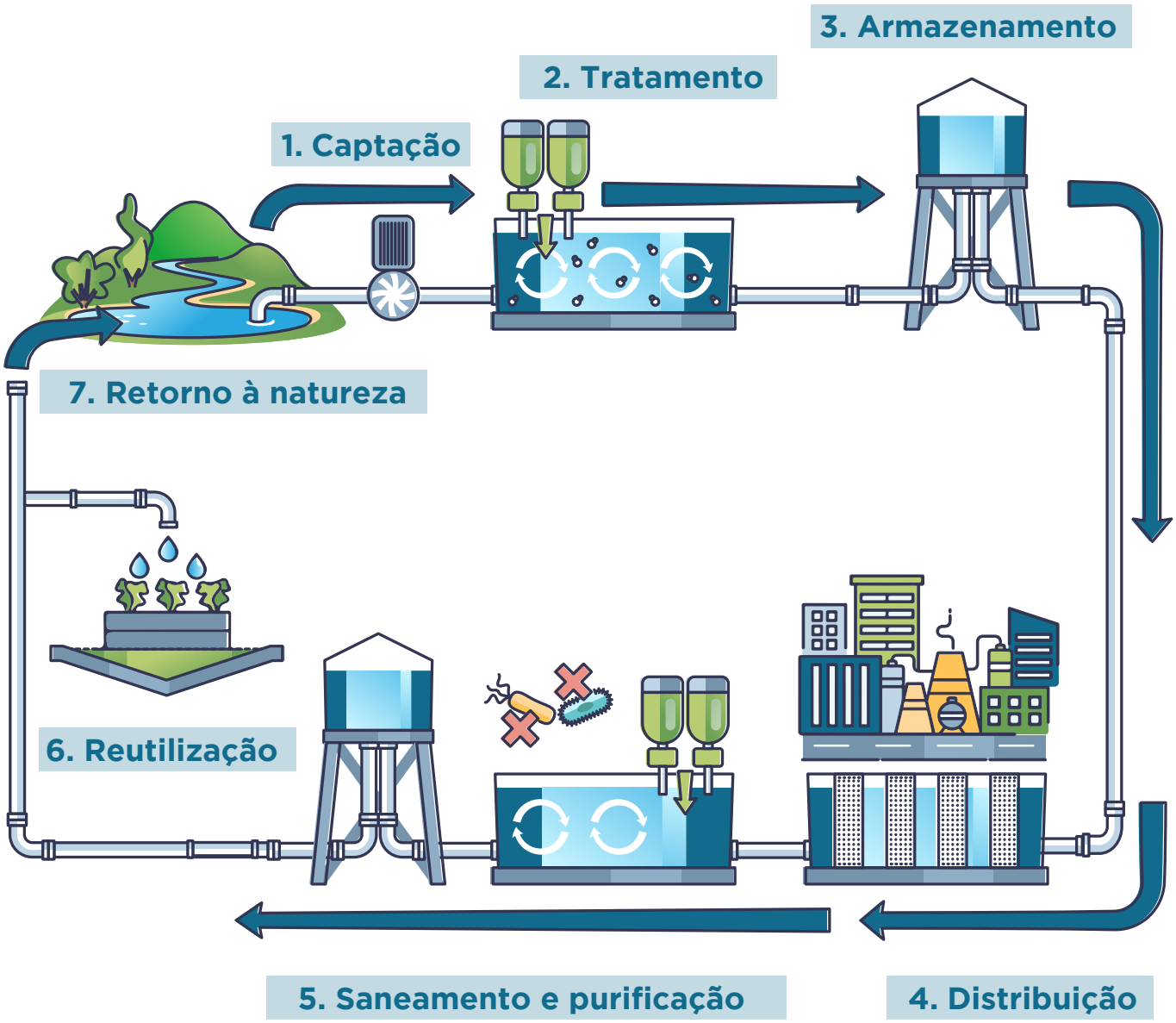
Tabela 2: Por que a indústria 4.0 é importante para o setor de A&S

Fatores	Descrição
Força de trabalho em processo de envelhecimento	A indústria da água está passando por uma mudança geracional em sua força de trabalho. Muitas pessoas estão se aproximando da aposentadoria, se aposentando ou deixando o setor por melhores oportunidades. Sua partida esgota a força de trabalho, mas o mais desconcertante é a perda de seu conhecimento e experiência indocumentados. Devido ao declínio das receitas, orçamentos apertados e imaturidade tecnológica, muitos dos melhores e mais brilhantes não são atraídos para a indústria da água, então os cargos podem ser preenchidos com recursos abaixo do ideal ou deixados em aberto.
Gestão de ativos	Os ativos em muitas empresas de abastecimento de água são antigos e precisam de reabilitação ou substituição. Espera-se que os orçamentos de capital diminuam nos próximos anos. Os custos operacionais estão disparando, pois os ativos frequentemente quebram e exigem reparos de emergência. Além disso, as práticas de gestão de ativos estão desatualizadas em comparação com indústrias como petróleo e gás, produtos químicos e serviços públicos de eletricidade.
Risco climático	As três primeiras revoluções industriais transformaram a sociedade moderna com a máquina a vapor, a era da ciência e da produção em massa e a ascensão da tecnologia digital, mudando fundamentalmente o mundo. Consequentemente, o planeta e seu clima também mudaram. Como resultado, os riscos estão aumentando para os aspectos ambientais, econômicos e sociais da civilização humana, desafiando a sociedade a encontrar novas maneiras de viver que sejam mais resilientes e sustentáveis. As concessionárias de água e as comunidades que elas atendem têm de enfrentar a diminuição do abastecimento de água, eventos de chuva mais frequentes e intensos, que exacerbam os transbordamentos combinados de esgoto (CSO) e transbordamentos de esgoto sanitário (SSO), e o aumento do nível do mar e a intrusão de água salgada.
Contaminantes emergentes	Microplásticos, compostos farmacêuticos e outros compostos refratários foram detectados em fontes de água potável, esgoto, lodo de águas residuais e biossólidos. Esses contaminantes são prejudiciais aos seres humanos e à vida aquática. A EPA dos Estados Unidos e suas agências ambientais estaduais exigirão, em breve, que as concessionárias de água monitorem e tratem ativamente esses contaminantes de acordo com os limites regulatórios pendentes.
Questões sociais	Incluem questões como crescimento populacional e migração, tanto internamente, do campo para as cidades, quanto internacionalmente.

Fonte: Mirjana *et al.* (2020).

A indústria 4.0 é necessária para a evolução do setor de A&S e sua maior eficiência. Mudar para a indústria 4.0 requer o uso de novas tecnologias digitalizadas na infraestrutura de água, o que a expõe mais do que nunca a ciberataques. A Figura 5 ilustra as várias etapas do tratamento de água.

Figura 5: Etapas do tratamento da água



Fonte: Aqualia Group (2019).

O impacto dos ciberataques na infraestrutura hídrica

O fornecimento de serviços de água e esgoto tem sido considerado um componente crítico do desenvolvimento econômico. A água é um recurso essencial para a sobrevivência das pessoas e do planeta. As interrupções nos sistemas de produção, transmissão e distribuição de água podem resultar em doenças e morbidade, prejudicar a agricultura e a indústria, ameaçar a segurança hídrica dos cidadãos e até minar a resiliência nacional. Portanto, os fornecedores de água devem sempre garantir o abastecimento de água estável e constante para minimizar possíveis danos à qualidade de vida dos cidadãos (Daigger *et al*., 2019).

A tríade CIA sobre segurança de dados

A tríade confidencialidade, integridade e disponibilidade, abreviada como CIA (da sigla em inglês: *confidentiality, integrity, availability*), foi criada para orientar as políticas de segurança digital das organizações em torno dos principais riscos cibernéticos. A confidencialidade limita o acesso a sistemas ou dados restritos apenas a usuários autorizados. A integridade garante a confiabilidade, precisão e integridade dos sistemas, processos ou dados. A disponibilidade garante acesso confiável aos sistemas ou dados (Wesley, 2023). Em muitos contextos de TI, a confidencialidade pode ser geralmente mais importante do que sua integridade, que, por sua vez, pode ser mais importante do que sua disponibilidade. No entanto, em ambientes centrados em ICS, essa ordem de importância é frequentemente invertida (Weiss, 2008): a disponibilidade extremamente alta do sistema e do serviço pode ser mais importante do que sua integridade, com a confidencialidade sendo relativamente menos importante, pois os contextos de ICS geralmente lidam com dados menos confidenciais.

Para ilustrar os princípios básicos de segurança da informação delineados pela tríade CIA, são exemplos de riscos para os sistemas de infraestrutura (Weiss, 2008):

1. Comprometimento da disponibilidade do sistema crítico, por exemplo, a capacidade de usar o sistema computadorizado crítico, conforme especificado, a qualquer momento e de qualquer local designado para esse fim.

2. Diminuição da capacidade crítica de produção do sistema.

3. Prejuízo da confiabilidade e integridade das informações ou processos críticos dos sistemas, com resultados contrários à finalidade pretendida. A alteração ou destruição não autorizada de informações pode prejudicar o bom funcionamento de sistemas informatizados críticos.

4. A violação da confidencialidade das informações armazenadas nesses sistemas pode afetar os sistemas informatizados críticos ou os ativos de informação da organização. Um exemplo pode ser a divulgação de dados usados por divisões comerciais em empresas de serviço público.

Elementos fundamentais que podem melhorar a postura de segurança cibernética do setor

De acordo com o relatório sobre o estado do setor de cibersegurança em 2021, publicado pelo Conselho Coordenador do Setor Hídrico dos Estados Unidos (WSCC, 2021), as quatro principais áreas de preocupação que afetam a cibersegurança do setor de A&S são lacunas em:

Uma publicação do Departamento de Energia dos Estados Unidos (Clark *et al.*, 2017) revela as cinco principais áreas técnicas do setor de A&S que sofrem com frequentes lacunas de segurança:

1. Configurações de rede
2. Proteção de mídia e plataformas de *streaming*
3. Acesso remoto a sistemas operacionais de água
4. Políticas e procedimentos documentados
5. Pessoal com treinamento inadequado

Uma pesquisa realizada pelo WSCC (2021) sobre o estado da cibersegurança para a infraestrutura hídrica nos Estados Unidos identificou necessidades para o setor, classificadas da mais necessária à menos necessária:

1. Suporte técnico
2. Subsídios ou empréstimos federais para equipamentos ou serviços de cibersegurança
3. Treinamento e formações orientados para o setor
4. Garantia da integridade da cadeia de suprimentos para hardware e software de TI e TO
5. Financiamento para contratar pessoal de cibersegurança
6. Informações sobre ameaças à cibersegurança

Rob Bates / Unsplash.com

De acordo com uma pesquisa realizada pelo Water Information and Sharing Analysis Center (WaterISAC, 2021) sobre o estado da cibersegurança da infraestrutura hídrica nos Estados Unidos, esta é uma amostragem representativa de sistemas de todos os tamanhos que fornece as seguintes alocações orçamentárias de 2021 para a cibersegurança:

- **38%** dos sistemas alocam menos de 1% do orçamento para a cibersegurança de TI
- **22,1%** dos sistemas alocam 1–5% do orçamento para a cibersegurança de TI
- **6,3%** dos sistemas alocam 6–10% do orçamento para a cibersegurança de TI
- **4,1%** dos sistemas alocam mais de 10% do orçamento para a cibersegurança de TI
- **44,8%** dos sistemas alocam menos de 1% do orçamento para a cibersegurança de TO
- **20,95%** dos sistemas alocam 1–5% do orçamento para cibersegurança de TO
- **4,9%** dos sistemas alocam 6–10% do orçamento para cibersegurança de TO
- **1,7%** dos sistemas alocam mais de 10% do orçamento para a cibersegurança de TO

Patrick Federi / Unsplash.com

Os números acima analisam relatórios de alocações orçamentárias na prática. Como tal, eles não indicam necessariamente a alocação ideal do orçamento de cibersegurança. Na verdade, eles podem documentar o orçamento insuficiente alocado para mitigar os riscos cibernéticos em instalações críticas e, especificamente, no domínio de TO.

Danos potenciais e seu impacto na infraestrutura hídrica

O impacto potencial na produção de água potável ou no tratamento de águas residuais pode incluir os seguintes cenários (Thielemann *et al.*, 2021):

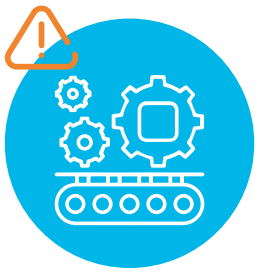
Os cidadãos seriam privados de água potável e saneamento

Hospitais não seriam capazes de funcionar

As mangueiras de incêndio não funcionariam

Escolas, escritórios e instalações governamentais seriam fechados

Culturas agrícolas seriam prejudicadas



Vários segmentos de manufaturas seriam interrompidos

O fornecimento de água seria interrompido nas instalações nucleares que dependem do resfriamento por meio de água

Todos os sistemas que lidam com abastecimento de água, qualidade da água, redução do risco de inundação, eletricidade, produção agrícola e águas residuais são potencialmente vulneráveis a ciberataques, com consequências drásticas para a saúde, o meio ambiente e a economia (Mission of Israel to the UN, 2021). A Tabela 3 apresenta possíveis cenários em que as ameaças cibernéticas às instalações de água envolvidas na produção, transmissão e purificação podem produzir prejuízos significativos (OECD Water, s.d.).

Tabela 3: Cenários de danos potenciais

Prejuízo potencial	Área(s) de impacto	Cenário 1	Cenário 2
Prejuízos ao fluxo funcional de produção e transmissão de água	• Uso urbano e doméstico • Produtividade industrial • Produtividade agrícola • Saúde humana	(a) Um jato de água de alta pressão pode fazer com que várias pedras e objetos que estão acima e ao redor do cano danificado voem, podendo prejudicar indivíduos e o meio ambiente.	(b) O vazamento de um cano de água subterrâneo causa deriva de areia, o que pode levar a danos às fundações, à infraestrutura subterrânea próxima, a estradas e edifícios, causando colapso e inundações.
Contaminação da fonte de água	• Público em geral	Manipulação do processo de purificação ou dessalinização da água.	CSO ou SSO causando contaminação maciça da água de poço.
Danos ambientais e ecológicos do tratamento de esgoto	• Produtividade agrícola • Saúde humana • Meio ambiente	As linhas de esgoto estão sob pressão hidráulica interna (linhas de drenagem) e, quando danificadas, podem causar danos às linhas de água. Normalmente, o fluxo nas linhas de esgoto depende da gravidade. Portanto, os principais riscos de danos à tubulação são a poluição ambiental, a contaminação de fontes de águas subterrâneas e os efeitos nocivos à saúde.	CSO ou SSO causando contaminação maciça da água de poço e problemas ambientais.

Fonte: autores e OECD Water (s.d.). Os cenários (a) e (b) são retirados de Ali e Choi (2019).

Harry Shelton / Unsplash.com

Preparação do setor de água e saneamento na América Latina e no Caribe

Cibersegurança regional na ALC

Tendências regionais

Os países diferem em sua abordagem à cibersegurança, dependendo de seu cenário econômico, político e cultural. Alguns países veem a cibersegurança como uma questão de segurança nacional, enquanto outros a veem como um desafio de desenvolvimento econômico. Como mencionado no relatório de cibersegurança do BID e da OEA, de 2020, a região da ALC não está suficientemente preparada para lidar com ciberataques. Apenas sete dos 32 países têm um plano de proteção de IC, enquanto vinte estabeleceram equipes de resposta a incidentes de cibersegurança. Isso limita sua capacidade de identificar ataques e reagir a eles.

O Modelo de Maturidade de Capacidade de Cibersegurança para Nações (CMM), desenvolvido pelo Centro Global de Capacidade de Segurança Cibernética da Universidade de Oxford (2021), é um modelo metódico projetado para revisar a capacidade de cibersegurança de um país. O CMM segue uma abordagem abrangente que avalia a maturidade das nações em cinco dimensões:

1. Política e estratégia de cibersegurança
2. Cibercultura e sociedade
3. Formação, treinamento e habilidades em cibersegurança
4. Marcos legais e regulatórios
5. Normas, organizações e tecnologias

O CMM foi utilizado pelo BID e pela OEA, em 2016 e 2020, para avaliar a maturidade dos países da ALC (BID e OEA, 2016 e 2020). De acordo com essas avaliações, os países da ALC progrediram em sua postura de cibersegurança: alguns dos países alcançaram níveis mais altos de maturidade nos indicadores de identificação, organização e gestão de riscos e resposta do aspecto de proteção de IC, entre outras melhorias relevantes. A principal tendência observada na região é o estabelecimento de planos de proteção de IC. Em 2016, apenas um em cada cinco países tinha uma estratégia de cibersegurança ou um plano de proteção de IC. Até 2020, doze países da região haviam aprovado estratégias nacionais de segurança cibernética, sete tinham planos de proteção de IC, enquanto outros estavam melhorando suas capacidades naquele momento.

Houve aumento dramático no custo do cibercrime global. Conforme relatado pela McAfee em sua publicação "The hidden cost of cybercrime" (Lewis, 2020), os custos aumentaram mais de 50%, de 2018 a 2020, passando de US$ 600 bilhões para mais de US$ 1 trilhão. Um relatório de 2021 divulgado pela IBM Security revelou que o custo médio por incidente cibernético em grandes empresas, na América Latina, aumentou 52,4%, de 2020 a 2021, estabelecendo o custo médio de violação de dados em US$ 2,56 milhões na ALC, enquanto o custo médio por incidente globalmente foi de US$ 4,24 milhões.

Argentina, Brasil, Colômbia e México estão entre as maiores e mais digitalizadas economias da ALC. Consequentemente, esses países têm algumas das maiores superfícies de exposição a ciberataques, o que significa que têm mais ativos digitais que podem ser potencialmente atacados. O *ransomware* de criptografia tornou-se uma importante ameaça à IC na região, onde a maioria dos sistemas de automação industrial atacados foi encontrada no Brasil (0,9%), México (0,5%) e na Colômbia (0,4%), com números representando a porcentagem de computadores atacados por *malware* no mesmo país. Um número menor de ataques foram registrados na Argentina, no Chile, Equador, na Costa Rica, República Dominicana, no Panamá e Paraguai (Kaspersky, 2017a).

Proteção de infraestrutura crítica na região

As dimensões consideradas no CMM procuram fornecer uma avaliação do nível de maturidade da capacidade de cibersegurança de um país, atribuindo um estágio específico que corresponde ao seu grau de obtenção de cibersegurança. Os cinco estágios de maturidade, que são atribuídos por meio de uma avaliação, variam do mais básico (inicial) ao mais avançado (dinâmico).

Figura 6: Cinco estágios de maturidade

Inicial

Nesta fase, ou não existe maturidade de cibersegurança, ou ela é de natureza muito embrionária. Pode haver discussões iniciais sobre a capacitação em cibersegurança, mas nenhuma ação concreta foi realizada. Há ausência de evidência observável da capacidade de cibersegurança nesse estágio.

Formativo

Alguns aspectos começaram a ser formulados e a se desenvolver, mas podem ser *ad hoc*, desorganizados, mal definidos – ou simplesmente novos. No entanto, evidências desse aspecto podem ser claramente demonstradas.

Estabelecido

Os elementos do aspecto estão em vigor e funcionando. No entanto, não há uma consideração bem pensada sobre a alocação relativa de recursos. Poucas decisões de compromisso foram realizadas no que diz respeito ao investimento relativo nesse aspecto. Mas o aspecto é funcional e definido.

Estratégico

Nesta fase, foram feitas escolhas sobre quais indicadores do aspecto são mais importantes e quais são menos importantes para a organização ou estado em particular. O estágio estratégico reflete o fato de que essas escolhas foram feitas, condicionadas às circunstâncias particulares do estado ou da organização.

Dinâmico

Neste estágio, existem mecanismos claros posicionados para alterar a estratégia, dependendo das circunstâncias prevalecentes, como a sofisticação tecnológica do ambiente de ameaça, um conflito global ou uma mudança significativa em uma área de preocupação (por exemplo, cibercrime ou privacidade). Organizações dinâmicas desenvolveram métodos para mudar estratégias rapidamente. Tomadas rápidas de decisão, realocação de recursos e atenção constante ao ambiente em mudança são características deste estágio.

Fonte: BID e OEA (2020).

Quando essa estrutura é aplicada para avaliar a proteção de IC nos países da ALC, é possível avaliar a capacidade de cada governo de **identificar** seus ativos de IC, engajar esforços **organizacionais** para regular a cibersegurança da IC mencionada anteriormente e as capacidades de **gestão e resposta a riscos,** reconhecendo a capacidade do país de proteger sua IC contra ameaças cibernéticas.

A Tabela 4 mostra a maturidade do país da ALC na proteção de IC, de acordo com o estudo de 2020 realizado pelo BID e pela OEA.

Tabela 4: Maturidade CMM do país na proteção de IC para a ALC

	Proteção de infraestrutura crítica														
País	**Identificação**					**Organização**					**Gestão e resposta a riscos**				
Antígua e Barbuda		2					2				1				
Argentina		2					2					2			
Bahamas		2				1					1				
Barbados	1					1					1				
Belize	1						2				1				
Bolívia		2				1					1				
Brasil			3					3					3		
Chile		2					2					2			
Colômbia			3						4					4	
Costa Rica	1					1					1				
Dominica	1					1					1				
Equador	1					1						2			
El Salvador	1					1					1				
Granada	1					1					1				
Guatemala	1					1					1				

	Proteção de infraestrutura crítica														
País	Identificação					Organização					Gestão e resposta a riscos				
Guiana		2				1					1				
Haiti	1					1					1				
Honduras		2					2					2			
Jamaica		2				1					1				
México		2					2					2			
Nicarágua	1					1					1				
Panamá		2					2					2			
Paraguai	1					1					1				
Peru		2					2				1				
República Dominicana	1						2				1				
São Cristóvão e Neves		2				1					1				
Santa Lúcia	1					1					1				
São Vicente e Granadinas	1					1					1				
Suriname	1					1					1				
Trinidad e Tobago		2					2					2			
Uruguai		2						3					3		
Venezuela	1					1						2			

Fonte: BID e OEA (2020).

Este estudo fornece uma visão crítica sobre a situação dos países da ALC individualmente e as oportunidades que a região como um todo pode capitalizar para melhorar sua proteção de IC. Com base nessas informações, destacamos que **o nível médio de maturidade da região ainda está entre 1 e 2** de acordo com o CMM. Em outras palavras, a maioria dos países da ALC acaba de começar a formular algumas iniciativas de cibersegurança envolvendo sua IC, com algumas dessas estratégias já em vigor. No entanto, elas estão sendo implementadas de forma *ad hoc*, sem coordenação entre as principais partes interessadas. Nesse sentido, os riscos associados à falta de um mecanismo institucionalizado para enfrentar as vulnerabilidades da IC apenas intensificam a capacidade de resposta interna da região, incluindo a organização de proteção de IC, a gestão de crises e a gestão e resposta a riscos – que, como resultado, se situam, em média, na base (BID e OEA, 2020).

Por que a ALC é mais vulnerável a ciberataques?

Assim como outras regiões globais, a ALC tornou-se cada vez mais digitalizada. Na última década, o acesso à internet na ALC aumentou exponencialmente (Prado, 2011). De acordo com a União Internacional de Telecomunicações (ITU, da sigla em inglês), mais de dois terços da população da ALC está on-line, em comparação com apenas 53,6% dos usuários da internet em todo o mundo (ITU, 2019). O aumento da penetração da internet nos domicílios ocorreu simultaneamente com o crescimento da digitalização de empresas, fábricas e prestadores de serviços, o que exigiu uma estratégia de cibersegurança mais madura, abrangente e relevante para a região.

Ao descrever o cenário de ameaças ao cibercrime na ALC, um fator é especialmente importante: o nexo entre desenvolvimento econômico, digitalização, governança e crime. Enquanto os países da ALC estão incorporando cadeias de suprimentos globais e continuando seu desenvolvimento econômico, o progresso institucional está correndo atrás. As fragilidades institucionais em alguns países resultam em uma governança de cibersegurança prejudicada, como na falta de uma legislação forte sobre crimes cibernéticos, aplicação adequada da lei cibernética, conhecimento técnico especializado e cooperação jurídica internacional. Isso, por sua vez, poderia atrair cibercriminosos que acreditam que a região é um alvo fácil (Pimenta Klein e Boguslavskiy, 2020).

Como outros tipos de crime, as características específicas do cibercrime na ALC estão relacionadas principalmente à vulnerabilidade socioeconômica em toda a região. Dada a disponibilidade de tecnologias digitais que permitem a fácil condução de crimes cibernéticos, os grupos criminosos tradicionais decidiram recorrer a atividades cibernéticas para ganhos financeiros potencialmente maiores em um domínio digital mal regulado, resultando em menores riscos para os criminosos.

Em outras palavras, o cibercrime na ALC é definido por fragilidades de desenvolvimento regional, ou seja, sua rápida digitalização e adaptação às novas tecnologias diante da regulamentação e política atrasadas. Esse vácuo de execução e autoridade criado pela expansão e evolução do uso de TIC atrai atores maliciosos, como grupos criminosos tradicionais. Como resultado, os atores de ameaças encontram inúmeras lacunas nas infraestruturas digitais e sociais e, portanto, são motivados a se envolver em atividades de cibercrime de uma forma quase sem reservas (Pimenta Klein e Boguslavskiy, 2020).

Por que não há mais ciberataques aos serviços públicos de água na ALC?

Como já mencionado, a infraestrutura hídrica na região da ALC é frequentemente antiga e ainda não mudou para sistemas tecnológicos avançados. Os sistemas de infraestrutura que não são digitalizados ou conectados on-line estão isolados de muitos riscos cibernéticos. No entanto, dois pontos importantes devem ser considerados quando se fala sobre o número de ciberataques a serviços públicos de água na região da ALC:

À medida que o setor de A&S adere a tecnologias mais avançadas, a previsão é que veremos mais ciberataques às concessionárias de água, até que mecanismos adequados de cibersegurança sejam implementados.

A falta de monitoramento cibernético de serviços de água já atualizados cria "pontos cegos", nos quais podem ocorrer ciberataques dos quais ainda não estamos cientes.

Cooperação regional em matéria de cibersegurança

Nas últimas décadas, a América Latina como região tem cooperado em questões de cibersegurança e fortalecido a capacidade dos países da região de combater ameaças digitais. Embora essa cooperação regional possa promover a convergência da diplomacia cibernética, os países da ALC até agora não formaram um bloco regional em diálogo com as Nações Unidas sobre a estabilidade do ciberespaço. As políticas e os mecanismos de proteção de segurança cibernética têm sido desenvolvidos lentamente pelos países da ALC, desde que foram a primeira região a articular uma estratégia de cibersegurança em 2004 (Van Raemdonck, 2020).

O Instituto de Estudos de Segurança da União Europeia identificou as causas dessa situação nos seguintes fatores:

1. Níveis desiguais de penetração digital
2. Pouco senso de urgência dos formuladores de políticas na coordenação de suas respostas de cibersegurança, devido à falta de divulgação pública de ataques de grande visibilidade
3. Falta de recursos financeiros para investir em segurança digital nacional
4. Falta de conhecimento técnico por parte dos formuladores de políticas e profissionais de TI

Outras razões para o lento progresso da ALC em se ajustar ao aumento das ameaças à cibersegurança são sua consciência limitada das medidas e riscos, a falta de confiança entre e dentro dos países da região, a desconexão entre os setores público e privado e disparidades socioeconômicas significativas, o que significa que mais pessoas caem no crime e, mais especificamente, no cibercrime. O Instituto de Estudos de Segurança da União Europeia reconhece que existem mecanismos eficazes de cooperação regional que podem ajudar a região a lidar com as ameaças digitais. Organizações multilaterais como o BID e a OEA contribuem para essa cooperação efetiva por meio de diferentes programas, gerenciados por seus grupos de cibersegurança.

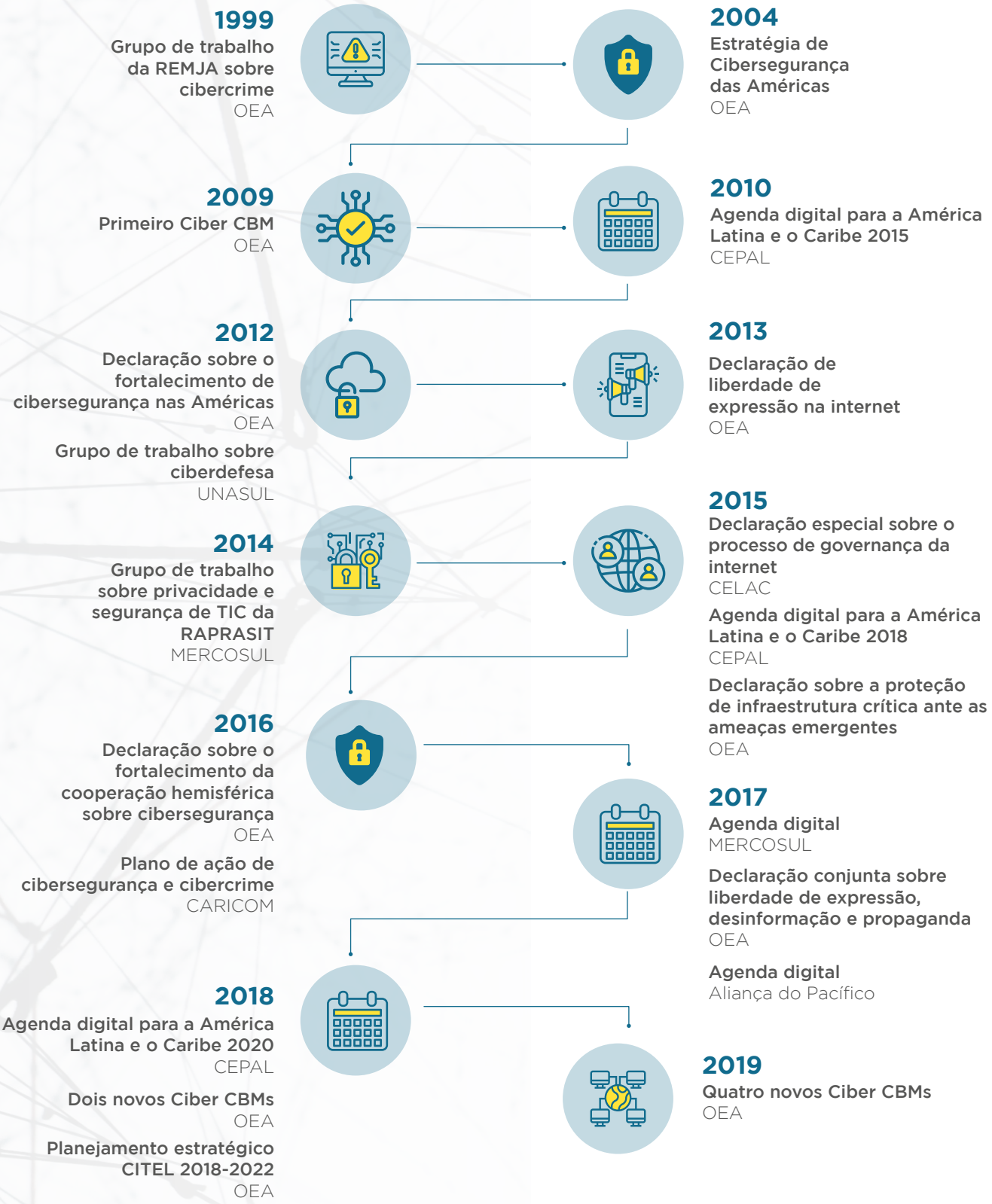
A evolução da cibersegurança no setor privado está ocorrendo principalmente graças à disponibilidade de recursos financeiros, humanos e tecnológicos. Por conseguinte, é necessária a cooperação entre os setores público e privado. Isso poderia ser realizado por meio de parcerias público-privadas (PPP), para promover políticas de cibersegurança nos níveis nacional, regional e internacional. Esse tipo de PPP requer uma boa coordenação e autoridade de tomada de decisão para lidar com ameaças cibernéticas.

Como os ciberataques podem atravessar fronteiras nacionais, a cooperação transnacional é crucial no domínio cibernético. As políticas cibernéticas devem ser atualizadas e coordenadas regionalmente, e os países devem investir esforços e recursos nesse campo comum (Saavedra, 2015). Organizações regionais e sub-regionais como a OEA, a União das Nações Sul-Americanas (UNASUL), o Sistema de Integração Centro-Americana (SICA) e outras podem ajudar a harmonizar estratégias para a cibersegurança comum da região, o que promoverá a legislação e a cooperação dos estados da região, bem como planos operacionais coerentes (Saavedra, 2015).

Falta de incentivos

Como o uso mundial de sistemas digitais passou por um aumento acentuado nos últimos anos, a crise de defesa cibernética agravou-se, e os ciberataques aumentaram dramaticamente. No entanto, outra explicação para o aumento do número de ciberataques é que não foram investidos recursos suficientes para desenvolver produtos e serviços seguros de hardware e software que operam no ciberespaço. Para a maioria das empresas, investir na cibersegurança de seus produtos pode não ser financeiramente viável, pois pode custar mais do que o dano potencial de incidentes de cibersegurança envolvendo seus produtos. Isso, por sua vez, leva a poucos incentivos para esse tipo de investimento (Brangetto e Kert-Saint Aubyn, 2015). Uma pesquisa com proprietários e operadores de IC, realizada pela OEA e pela Microsoft, em 2018, descobriu que muitos governos da região não estabeleceram programas de incentivo para encorajar esses proprietários e operadores a adotar voluntariamente medidas de cibersegurança, nem começaram a implementar frameworks obrigatórios (OEA, 2018). A figura a seguir fornece uma visão geral de vinte anos de iniciativas na região da ALC.

Figura 7: Iniciativas de política de cibersegurança na ALC 1999–2019



Fonte: Van Raemdonck (2020).
Notas: REMJA: Reuniões de Ministros da Justiça ou de Outros Ministros ou Procuradores-Gerais das Américas; CITEL: Comissão Interamericana de Telecomunicações; RAPRASIT: Reunião de Autoridades sobre Privacidade e Segurança da Informação e Infraestrutura Tecnológica.

Entrevistas: metodologia e perspectivas

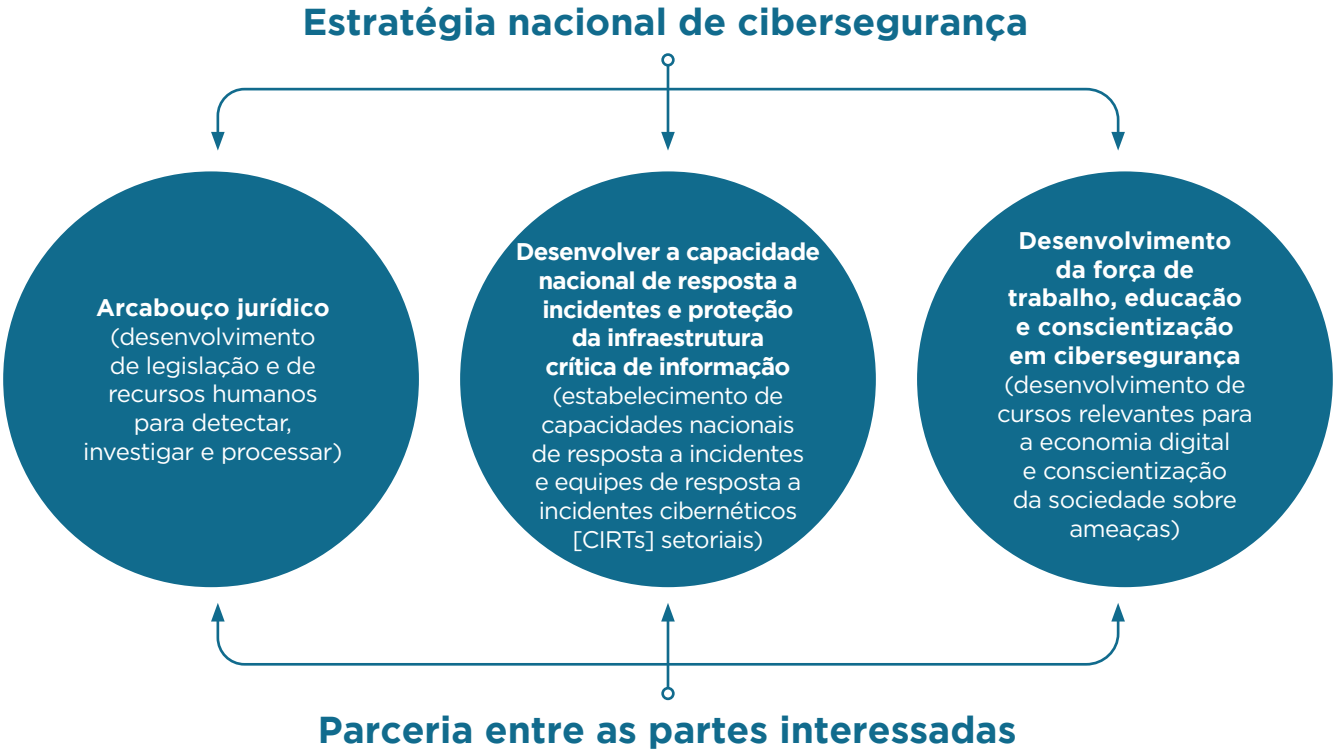
Para aprimorar ainda mais nosso relatório, realizamos várias entrevistas na região, com representantes de instituições em nível estatal, bem como serviços públicos de água em sete países: Belize, Brasil, Chile, Jamaica, Panamá, Suriname e Trinidad e Tobago. As entrevistas foram realizadas por meio de videochamadas on-line, e cada entrevistado foi questionado sobre cibersegurança na região, em seu país específico e no setor de A&S (ver Apêndices A e B).

Os países da região da ALC demonstraram esforços para melhorar a proteção da cibersegurança de sua infraestrutura hídrica, mas as proteções existentes não abordam totalmente os riscos. Esse processo requer regulamentação adicional, financiamento, bem como maior conscientização das instalações fornecedoras de água pelos proprietários e operadores.

A partir das entrevistas, identificamos várias tendências, incluindo o aumento do investimento em cibersegurança, já que a administração reconheceu que os riscos cibernéticos afetam uma variedade de domínios operacionais, como o comercial, o tratamento de águas residuais, os recursos hídricos e a qualidade dos serviços. Embora alguns aspectos como a qualidade do abastecimento de água sejam fortemente regulamentados, a regulamentação dos aspectos de cibersegurança muitas vezes é incompleta.

Em alguns países da ALC, a maioria dos processos operacionais ainda está sendo realizada manualmente, com apenas 15% dos sistemas operados por suas autoridades de água sendo gerenciados remotamente. Essas tendências podem ser vistas no caso de Belize (Belize Crime Observatory, 2020) conforme descrito na Figura 8.

Figura 8: Prioridades na estratégia de cibersegurança de Belize 2020-2030



Fonte: Ministério do Interior de Belize (2020).

O segundo objetivo descrito na estratégia nacional de Belize, publicada em 2020, refere-se a padrões mínimos de segurança para sistemas de IC de informação. Espera-se que o objetivo seja alcançado no longo prazo e inclua várias atividades. Entre eles (Belize Crime Observatory, 2020):

1. Identificar padrões mínimos para IC de informação.

2. Desenvolver padrões mínimos de segurança para sistemas críticos de infraestrutura de informação.

3. Estabelecer um grupo de trabalho com a incumbência de analisar ameaças e recomendar padrões de acordo com a indústria.

Cibersegurança no setor de água e saneamento na ALC

Questões adicionais também foram identificadas com base nas entrevistas, conforme segue:

Falta de designação oficial da infraestrutura hídrica como crítica. Uma questão que dificulta os esforços mais extensos dos órgãos estatais oficiais para melhorar a cibersegurança da infraestrutura hídrica é a falta de uma designação oficial como IC nacional. Isso está relacionado principalmente à fraca gestão nacional de riscos cibernéticos de IC em alguns países.

Equipes internas de cibersegurança da empresa insuficientes, à medida que as concessionárias de água se digitalizam. Algumas organizações de água da ALC atualmente usam guias genéricos de "melhores práticas" da indústria e dos fornecedores sobre cibersegurança (por exemplo, políticas de *firewall*) e ainda não estabeleceram seus próprios guias. Isso pode se dever ao fato de a digitalização dos sistemas de água nesses países ser relativamente nova e estar em andamento, embora alguns desses países compartilhem informações e conhecimentos sobre soluções de cibersegurança para as indústrias de água no mercado interno. Em alguns casos, isso pode ser feito de maneira oficialmente estruturada, enquanto em outros pode ser feito de maneira informal, com base em relacionamentos pessoais.

Falta de entidades designadas para cibersegurança. Outra questão que impede os países de ter uma forte estratégia de cibersegurança para IC de água é a falta de uma entidade designada responsável por essa questão dentro das agências de água do país. Por exemplo, em um dos países da ALC, uma empresa pública responsável pelo abastecimento de água não tem uma função dedicada à cibersegurança. As operações cibernéticas diárias nessa organização estão sendo realizadas pelo departamento de TI, cujos funcionários representam menos de 1% do número total de funcionários do provedor de água.

Ameaças novas e ainda não conhecidas. Alguns países da ALC têm mecanismos mais avançados para gerenciar a cibersegurança de IC, mas continuam despreparados para um ataque sério contra suas instalações de água. Questões que afetam a preparação incluem experiência limitada em lidar com grandes ataques e disponibilidade limitada de profissionais altamente especializados necessários. Em um dos países mais maduros da ALC em termos de cibersegurança, o maior provedor de serviços de água e esgoto reconhece que as áreas mais significativas de preocupação enfrentadas pelo setor são a falta de conhecimento em torno do inventário total de dispositivos de TI e TO, infraestrutura industrial não segura (ou seja, ativos digitais) e falta de treinamento de pessoal. Do ponto de vista deles, isso poderia ter impacto sobre:

Em outro exemplo, um dos fornecedores de água que participou das entrevistas é regulamentado por duas autoridades: uma para a qualidade do serviço e outra para as questões tecnológicas. Embora a regulamentação seja um passo importante para uma forte defesa cibernética, a organização tem apenas um funcionário no departamento de TI responsável pela cibersegurança. Além disso, a organização não possui procedimentos de cibersegurança aprovados, para além de uma lista de tarefas e da necessidade de verificar os controles básicos. Os controles, no entanto, não são regulamentados e são revisados dependendo apenas de sua criticidade. A organização também não possui um plano de trabalho anual abrangente de cibersegurança – ela gerencia apenas uma lista de projetos de cibersegurança, avaliados anualmente. Também nunca realizou uma auditoria de cibersegurança, embora um teste de penetração tenha sido feito quatro anos antes da entrevista. Foi revelado que usou metodologias para proteger dispositivos de TO em outros setores e os adaptou à indústria da água.

Descrição do status de cibersegurança em cinco países

Medidas específicas por país

Vários exemplos de países da ALC e sua abordagem para melhorar a resiliência de cibersegurança de seu país são fornecidos abaixo.

Argentina

Nos últimos anos, a Argentina tomou várias medidas para implementar políticas, regulamentos e reformas nos setores de telecomunicações, internet e tecnologia do país (BID e OEA, 2020). Em 2008, o país alterou o código penal para incluir o cibercrime. Em 2016, o poder executivo emitiu um decreto criando o Ministério da Modernização. O decreto estabeleceu a Subsecretaria de Tecnologia e Segurança Cibernética dentro do novo ministério e a colocou a cargo do Escritório Nacional de Tecnologia da Informação, da Diretoria Nacional de Infraestrutura e Operações e da Diretoria Nacional de Infraestrutura Crítica de Informação e Segurança Cibernética (Privacy International, 2019). Em 2017, o Comitê de Cibersegurança foi estabelecido sob o Gabinete de Ministros e incluiu representantes dos Ministérios da Defesa e Segurança. Sua missão era desenvolver uma estratégia nacional de cibersegurança, que foi publicada em 2019. O Decreto 50 de 2019 atribuiu responsabilidades em matéria de proteção de IC ao Secretário de Inovação Pública no Gabinete dos Ministros. No início de 2023, esse mesmo escritório realizou consultas públicas para atualizar a Estratégia Nacional de Cibersegurança.

A Argentina foi um dos primeiros países da ALC a ter um marco regulatório para proteção de dados pessoais e é um dos poucos países das Américas que participa da Convenção do Conselho da Europa para a Proteção de Indivíduos no que diz respeito ao Tratamento Automático de Dados Pessoais. O governo argentino recebeu um empréstimo baseado em políticas (PBL) do BID em 2019 para apoiar a implementação de políticas relacionadas a infraestrutura e práticas críticas no uso de TIC em seus esforços para fortalecer as capacidades nacionais de cibersegurança e outro empréstimo de investimento do BID em 2023 para proteger a IC de informações. A Argentina também estabeleceu um Programa Nacional de Infraestruturas Críticas para Informação e Cibersegurança (ICIC) para construir um marco regulatório que defina e proteja a infraestrutura estratégica e crítica pertencente aos setores público e privado, bem como às organizações interjurisdicionais. Também vale ressaltar que a Argentina oferece diversas oportunidades educacionais para a educação cibernética em universidades públicas e privadas, bem como na sociedade civil, e pertence a grupos de trabalho de segurança cibernética com países estrangeiros (BID e OEA, 2020).

Brasil

Os operadores de IC pública e privada no Brasil variam em sua maturidade na proteção de IC. As avaliações de risco de cibersegurança devem ser realizadas anualmente por todas as instituições federais com base nas lições aprendidas com os principais incidentes cibernéticos. Em resposta às informações fornecidas pela ferramenta de conscientização situacional da equipe de resposta a emergências informáticas do Brasil (CERT.br), todas as instituições públicas possuem políticas e procedimentos claramente definidos em vigor (OEA, 2020). Cerca de 54% dos ciberataques relatados no Brasil são originários de dentro do país (Lewis, 2018).

Chile

Ao contrário de seus vizinhos sul-americanos, o cibercrime mais comum no Chile não é fraude ou *phishing*, mas infecção por *malware*. Essa tendência é o resultado de uma população tecnicamente cibereducada que faz uso das melhores práticas para manter seus dispositivos e dados seguros. Os alvos, no entanto, são como os de outros países latino-americanos: o setor financeiro, especialmente os bancos. Para ilustrar isso, o Banco do Chile, o segundo maior banco do país, sofreu um grande ataque de *ransomware* em maio de 2018 e perdeu US$ 10 milhões (Pimenta Klein e Boguslavskiy, 2020). O Chile publicou sua Política Nacional de Cibersegurança, incluindo medidas para proteger IC em 2017. Uma versão atualizada está sendo elaborada em 2023.

Colômbia

A Colômbia foi o primeiro país latino-americano a aprovar uma estratégia nacional de cibersegurança em 2011. Cinco anos depois, implementou uma estratégia atualizada conhecida como Política nacional de segurança digital. Essa nova versão atualizou a visão da primeira política, dessa vez incluindo a gestão de riscos (Hernández, 2018). Em 2023, o Plano Nacional de Desenvolvimento 2023–2026 destacou a importância da proteção da IC e estabeleceu que uma Diretoria Nacional de Segurança Digital coordenaria esses esforços, conforme estabelecido no Decreto 338 de 2022.

República Dominicana

De acordo com um estudo sobre o nível de maturidade das estratégias nacionais de cibersegurança, a estratégia da República Dominicana é considerada uma das mais maduras da ALC, classificada pelo modelo como consolidada. A partir de 2020, avaliou-se que a estratégia e a política de cibersegurança do país apresentava fraquezas relativas na gestão de crises, defesa cibernética e redundância de comunicações, áreas nas quais avanços subsequentes foram feitos. Em termos de proteção de IC, a República Dominicana é mais forte em aspectos organizacionais, enquanto os aspectos de identificação e gerenciamento de risco e resposta estão sendo aprimorados (BID e OEA, 2020).

Como mostrado nos exemplos anteriores, os cinco estudos de caso sobre estratégia e regulamentação nacionais de cibersegurança não tratam especificamente de cibersegurança na infraestrutura hídrica. A seção a seguir discutirá dois estudos de caso de Israel e do Reino Unido, apresentando suas estratégias nacionais em termos gerais e, especificamente, sua regulamentação para a cibersegurança da infraestrutura hídrica.

Erik Mclean / Unsplash.com

Desafios e respostas em nível internacional

Os países ao redor do mundo certamente estão cientes dos vários riscos potenciais de operar no ciberespaço, incluindo os possíveis danos que os ciberataques podem infligir à economia e à vida civil, e até mesmo considerando casos em que os atores tentam avançar seus objetivos geoestratégicos por meio de interrupções on-line, representando riscos significativos para a IC nacional. À medida que esse entendimento cresce, os países estão investindo mais esforços voltados para os controles nacionais de cibersegurança e segurança para sistemas ciberfísicos que sustentam os esforços de missão crítica (Thielemann *et al.*, 2021).

Entendendo a importância das parcerias público-privadas

Como as IC são de propriedade de atores públicos e privados e por eles operadas, e os ataques podem ter efeitos abrangentes, a responsabilidade de protegê-las está nas mãos de entidades do setor público e privado. No entanto, o foco principal dos dois setores é diferente. O setor público vê a infraestrutura em nível nacional e tende a colocar maior esforço nos ativos mais estratégicos. Por essa abordagem, os governos abordam a proteção de IC como uma coleção de sistemas e serviços.

Já o setor privado prioriza seus lucros, posição e clientes, o que o leva a atribuir maior valor à prestação de serviços, inovação, redução de custos e construção de participação de mercado. No nível técnico, o setor privado coloca seus esforços na direção de elementos centrais dentro de seu controle direto ou de suas obrigações contratuais de prestação de serviços.

Essas diferentes abordagens criam oportunidades para parcerias público-privadas nos níveis estratégico e técnico para superar essas diferenças e proteger a IC de maneira holística. As organizações privadas devem se esforçar para entender seu papel na proteção de IC, enquanto os governos devem apreciar o conhecimento especializado disponível no setor privado (OEA, 2018).

Estudos de casos internacionais

Para entender como os governos podem proteger sua IC contra ameaças cibernéticas, com foco no setor de A&S, apresentamos dois estudos de caso envolvendo Israel e o Reino Unido. Os dois modelos aqui descritos ilustram os regulamentos em nível nacional estabelecidos para lidar com os riscos de cibersegurança.

Estudo de caso 1: o modelo israelense

O governo de Israel tem abordado questões que envolvem a segurança da informação e a proteção da infraestrutura informatizada há quase três décadas. Desde 1996, tem aprovado medidas de defesa contra ameaças cibernéticas (Tabansky, 2011). Em Israel, há ênfase significativa na regulação e coordenação entre os setores público e privado. Logo no início, o país designou o setor de A&S como IC e tem sido ativo na conscientização dos riscos associados. Além disso, as autoridades cibernéticas do governo alocam recursos em nível nacional para realizar revisões periódicas, exercícios e treinamento, promovendo assim a importância de se concentrar em capacidades para proteger a infraestrutura hídrica. Essas iniciativas incentivam as entidades privadas relevantes a melhorar suas medidas de proteção e resposta.

Regulamento

O modelo israelense para proteger a infraestrutura contra ameaças cibernéticas é centralizado, no qual um órgão de supervisão analisa de perto as atividades de segurança dos operadores de infraestrutura, emitindo instruções diretas para as medidas a serem tomadas conforme necessário. Em 2002, o governo israelense procurou definir responsabilidades para os sistemas informatizados do país, incluindo o estabelecimento de um comitê diretor que determinasse quais órgãos seriam definidos como críticos e, portanto, exigiriam proteção e diretrizes cibernéticas (Benoliel, 2014). Em 2010, o governo estabeleceu sua autoridade nacional de segurança cibernética, atualmente conhecida como Israel National Cyber Directorate (INCD). O INCD trabalha para formular uma política abrangente de proteção do ciberespaço para Israel, lidando com a supervisão e regulamentação das atividades do governo geral relacionadas ao ciberespaço do ponto de vista da segurança civil e nacional (Benoliel, 2014).

Sob sua responsabilidade regulatória, o Ministério de Energia e Água de Israel, o gabinete do governo responsável pela infraestrutura de energia e água, trabalha com instalações de infraestrutura privada para proteger sistemas críticos de computadores. Os procedimentos elaborados pelo Ministério orientam as instalações privadas de infraestrutura (por exemplo, gás e eletricidade) na proteção dos sistemas digitais críticos que operam.

A Autoridade de Água e Esgoto, fundada em 2007, é responsável pela operação do sistema de abastecimento de água nos níveis nacional, distrital e local. A missão da Autoridade de Água e Esgoto é preservar as fontes de água e manter as operações de abastecimento, bem como responder a eventos de emergência, como aqueles que possam prejudicar a infraestrutura hídrica.

A Unidade de Segurança Hídrica opera em nome da Autoridade de Água e Esgoto na questão da cibersegurança e lida com operações, gestão e controle de incidentes de danos físicos e digitais à água, bem como crises de água. A unidade também é responsável por melhorar as capacidades dos ministérios governamentais, das agências nacionais e dos fornecedores de água (usinas de dessalinização, usinas de água, empresas de abastecimento de água) e está envolvida na preparação para

incidentes do setor de A&S, organizando, fornecendo equipamentos, elaborando procedimentos e praticando e mantendo os padrões operacionais necessários.

A Autoridade de Água e Esgoto de Israel definiu uma escala para o nível de proteção cibernética necessário para os fornecedores de água. Usando essa escala, cada fornecedor de água determina seu próprio nível de sensibilidade, o que consequentemente determina os controles de cibersegurança necessários, da forma a seguir.

Instalação ou infraestrutura de nível 1:

A. Instalações de abastecimento de água ou infraestrutura cujos danos perturbarão a continuidade funcional do abastecimento de água para uma população de mais de 250.000 habitantes.
B. Usina de dessalinização.
C. Estações de tratamento de esgoto cuja interrupção pode causar danos ambientais graves e duradouros.

Instalação ou infraestrutura de nível 2:

A. Instalações de abastecimento de água ou infraestrutura cujos danos perturbarão a continuidade funcional do abastecimento de água para uma população de menos de 250.000 habitantes.
B. Instalações onde a autoprodução de água por meio de perfuração é realizada e há cloração.

Instalação ou infraestrutura de nível 3:

A. Uma instalação que não possui sistemas informatizados considerados essenciais para o funcionamento de suas operações de água e esgoto.

A Unidade de Segurança Hídrica tem autoridade exclusiva para elevar o nível determinado de criticidade para uma instalação com base em uma ponderação do leque de ameaças, o potencial de danos à continuidade funcional, mão de obra disponível, custos e muito mais.

Estudo de caso de ataque e resposta

Em abril de 2020, hackers maliciosos afiliados a interesses iranianos supostamente atacaram várias estações de bombeamento e instalações de tratamento de águas residuais em Israel, tentando manipular sistemas de cloro para aumentar as quantidades dessa substância na água fornecida à população de Israel (Srivastava, 2020). De acordo com informações publicadas, o ataque iraniano foi realizado por meio de servidores nos Estados Unidos e na Europa, a fim de esconder sua origem e reduzir as suspeitas. Atingiu controladores de software comuns, que estavam utilizando CLPs para operar bombas de água. Esses CLPs foram acessados pelos atacantes pela internet para controlar as bombas de água.

Foi relatado que o governo israelense respondeu rapidamente, ordenando que todas as instalações de água e energia do país redefinissem as senhas em todos os seus sistemas SCADA para evitar novos ataques. Graças à resposta rápida, não ocorreram danos significativos na qualidade da água (Boubaker, 2021). Decidiu-se, então, fortalecer os controles de segurança que protegem os sistemas SCADA, desconectando esses sistemas da internet, a fim de garantir a operação contínua dessas instalações.

Estudo de caso 2: o modelo do Reino Unido

Regulamento

O Reino Unido tem uma longa história de uso de ciência e tecnologia para fins de segurança nacional, e seu governo tem mantido uma estratégia e política de longo prazo para apoiar a inovação, a tecnologia e as indústrias intensivas em conhecimento. A Estratégia de Segurança Nacional Britânica (NSS), publicada em 2015, definiu as ameaças cibernéticas como uma categoria de ameaça superior e risco de alto nível para os interesses da Grã-Bretanha. Um ano depois, o Reino Unido publicou sua estratégia cibernética nacional para 2016-2021 e depois a atualizou para 2022-2030.

A estratégia de 2022 inclui cinco objetivos principais:

- Gerenciar riscos de cibersegurança
- Proteger contra ciberataques
- Detectar eventos de cibersegurança
- Minimizar o impacto de incidentes de cibersegurança
- Desenvolver habilidades, conhecimento e cultura de cibersegurança

O governo do Reino Unido está investindo maciçamente na realização do plano de trabalho para alcançar os objetivos estabelecidos na estratégia cibernética nacional. Somente em 2021, foram investidos £ 2,6 bilhões em cibersegurança. Essa atenção dada à cibersegurança decorre de uma série de ciberataques a instituições políticas, partidos e órgãos parlamentares, bem como ciberataques nos quais dados da infraestrutura nacional britânica foram roubados.

Um passo adicional para melhorar a cibersegurança é a reforma institucional cibernética britânica, que estabeleceu o Centro Nacional de Segurança Cibernética (NCSC, da sigla em inglês). O NCSC foi responsável pela implementação operacional governamental de toda a proteção da cibersegurança no Reino Unido, incluindo questões que anteriormente estavam sob a responsabilidade do Centro de Proteção da Infraestrutura Nacional.

Em 2017, o Departamento de Meio Ambiente, Alimentação e Assuntos Rurais divulgou a Estratégia de Cibersegurança do Setor de Água para 2017-2021. Seus objetivos foram guiados pela Estratégia Nacional de Cibersegurança (NCSS) descrita na Figura 9.

Figura 9: Estratégia nacional de cibersegurança do Reino Unido

Fonte: HM Government (2017).

Estudo de caso de ataque e resposta

Aproximadamente 40% dos 777 incidentes gerenciados pelo NCSC, entre setembro de 2020 e agosto de 2021, foram direcionados a entidades relacionadas ao governo no Reino Unido. Em maio de 2021, o Departamento Executivo do Serviço de Saúde irlandês sofreu um ciberataque. Foi anunciado que os custos de recuperação desse ataque seriam de US$ 600 milhões (HM Government, 2021).

Nesses casos, o NCSC desempenha vários papéis. Em primeiro lugar, em parceria com outros setores do governo, identifica os agentes de ameaça e atribui ataques a eles. Em segundo lugar, depois de detectar um incidente cibernético, o NCSC o analisa para avaliar suas características ("incidente de triagem NCSC"). Após essa avaliação, se for decidido que é necessária uma intervenção adicional do NCSC, o apoio é fornecido por uma equipe técnica e uma equipe jurídica. Mais tarde, o NCSC coordena com entidades internacionais, se necessário. Após incidentes, avaliações são compartilhadas e novos métodos para lidar com ataques semelhantes são apresentados (HM Government, 2021).

Nathan Roser / Unsplash.com

Principais recomendações para o setor de água e saneamento da América Latina e Caribe

Principais recomendações de cibersegurança

O movimento em direção à indústria 4.0 e a convergência resultante de TI e TO levou ao aparecimento de novas ameaças cibernéticas para o setor de A&S. Várias das organizações de água e saneamento entrevistadas para este estudo enfatizaram que planejam mais automação e digitalização de sua infraestrutura nos próximos cinco a dez anos. Com a crescente digitalização e automação de processos do setor de A&S, o estabelecimento de controles apropriados de cibersegurança é imperativo para aumentar a resiliência aos ciberataques e, assim, apoiar a confiabilidade, a qualidade e a segurança desses serviços.

A seguir, você encontrará uma série de recomendações que seguem os resultados de nossas pesquisas e entrevistas.

Garantir que os atores nacionais, subnacionais e locais descrevam claramente sua visão e definam metas para alcançá-la

1. Criar uma **visão de cibersegurança clara e viável** e detalhá-la em uma **estratégia governamental de cibersegurança de IC.** Essa visão deve incluir governança clara e capaz, **objetivos** bem definidos e **mensuráveis** e um roteiro para alcançá-los.

2. **Obter apoio e compromisso da liderança nacional do governo** para reforçar a cibersegurança do setor de A&S e outras IC, incluindo a liderança proativa da agência nacional de cibersegurança, fortalecendo os recursos humanos e técnicos disponíveis para o setor e estabelecendo governança clara e capacidades operacionais para regular e proteger a IC.

Criar um marco legal no qual o setor de água e saneamento seja reconhecido como infraestrutura crítica

1. O primeiro passo que precisa ser dado é o **reconhecimento formal do setor de A&S como IC**. Na maioria dos países da ALC, o setor de A&S não é oficialmente reconhecido como IC, muitas vezes um fator-chave necessário para que o setor receba o orçamento e a prioridade gerencial necessários em relação aos desafios de cibersegurança. Sem esse reconhecimento, o setor de A&S não receberá a atenção adequada e, mais especificamente, controles de cibersegurança insuficientes serão implementados.

2. Nos últimos anos, vários países da região da ALC modernizaram seus marcos regulatórios de cibersegurança, graças à sua conscientização cada vez maior sobre a crescente importância dessa questão, especialmente para sistemas de IC. No entanto, os esforços de legislação em nível nacional e subnacional em muitos dos países da ALC ainda não resultaram na implementação coerente de estratégias e planos de ação de cibersegurança. Foram introduzidas melhorias a esse respeito, mas as atividades devem ser aceleradas ainda mais. Assim, **a implementação coerente de estratégias e planos de ação de cibersegurança, com foco em IC, deve ser priorizada**.

3. Ao mesmo tempo, vários países da ALC fortaleceram suas estruturas institucionais para reduzir os riscos cibernéticos e melhorar a proteção e a resiliência quando esses riscos se materializam, incluindo investimentos em processos, pessoal e recursos tecnológicos. Tais **esforços e coordenação interinstitucional são necessários nos níveis nacional e internacional** (Saavedra, 2015).

Enzo Tommasi / Unsplash.com

Estabelecer e priorizar parcerias públicas e privadas para compartilhar conhecimento

1. A proteção de IC deve basear-se em **parcerias que reúnam atores privados e público-privados**. Para gerenciar melhor o risco, governos, proprietários e operadores de IC e fornecedores de TIC devem colaborar entre setores e fronteiras (OEA, 2018). Estratégias eficazes de segurança e resiliência de IC exigem parcerias público-privadas, que, por sua vez, tornam o **compartilhamento de informações oportuno e confiável entre as partes interessadas, o que é essencial para a proteção de IC** (CISA, 2022).

2. O compartilhamento de informações também aumenta o potencial de respostas coletivas a ameaças cibernéticas. As organizações estão mais bem preparadas para frustrar os invasores e os métodos de ataque quando as **informações sobre os cibercriminosos e seus métodos são compartilhadas**. Seria sensato que os governos considerassem a criação de estruturas e incentivos para encorajar as organizações de IC a participar dessa atividade (OEA, 2018).

3. As parcerias público-privadas são de extrema importância no setor de A&S, pois é um setor melhor descrito como "conservador", na medida em que possui muitos profissionais empregados na área hídrica, mas poucos especialistas em cibernética que possam lidar com aspectos de cibersegurança que afetem a área. Assim, **a criação de parcerias entre o conhecimento cibernético encontrado no setor privado e o conhecimento encontrado no setor de A&S pode expor o setor às melhores práticas da indústria e ao *know-how* em cibersegurança**.

4. As parcerias público-privadas podem ser eficazes para além do simples compartilhamento de informações acionáveis sobre ameaças. Os governos podem reunir diferentes partes interessadas para melhorar a segurança de seus serviços críticos, **formando grupos de trabalho ou comitês consultivos**. Suas áreas de foco podem incluir o estabelecimento de estruturas de coordenação eficazes e processos e protocolos de compartilhamento de informações, identificando e trocando ideias, abordagens e melhores práticas para aperfeiçoar a segurança e a coordenação internacional (OEA, 2018).

Helio Dilolwa / Unsplash.com

Compreender que as organizações e concessionárias dos serviços públicos e privados devem desenvolver culturas corporativas que enfatizem a cibersegurança

1. **Reconhecer a cibersegurança como um risco**, no mesmo nível de segurança, qualidade de serviço, proteção ambiental e outras prioridades operacionais.

2. **Aumentar a conscientização sobre cibersegurança**, criando uma cultura de cibersegurança com envolvimento da gerência (por exemplo, treinamento, exercícios de simulação de resposta a incidentes cibernéticos, cursos na área, etc.).

3. **Incorporar diretivas de segurança** para a IC na governança corporativa.

4. **Adaptar-se continuamente às mudanças.** O domínio do ciberespaço, incluindo tecnologias, ameaças e vulnerabilidades, muda rapidamente. Reconhecer e aceitar as mudanças aumentará o reconhecimento e a aceitação dos esforços do setor público e privado em nível nacional para criar resiliência cibernética.

Compreender que as organizações e serviços públicos e privados devem estabelecer e adaptar as etapas práticas dentro da organização a serem realizadas antes da implementação de controles de cibersegurança

1. **Mapear riscos e realizar avaliações de impacto**, modelando os impactos potenciais de ciberataques, incluindo aqueles na vida humana. Isso orientará a continuidade dos negócios corporativos e os esquemas de classificação de dados.

2. **Mapear e identificar os ativos, dispositivos e sistemas** envolvidos na rede TO/ICS.

3. **Criar um plano anual e orçamentado de cibersegurança** que inclua conscientização, treinamento específico para equipes relevantes, exercícios cibernéticos entre empresas e a manutenção e atualização necessárias de soluções de segurança.

4. **Preparar e treinar para o tratamento de incidentes e recuperação de desastres**, mantendo um plano atualizado de resposta a incidentes cibernéticos.

5. **Implementar requisitos de cibersegurança** em todos os processos comerciais e técnicos, compras, cadeia de suprimentos e prestadores de serviços.

Formular soluções de cibersegurança para a convergência de TI e TO de organizações e serviços públicos e privados

1. **Desenvolver uma estratégia de segurança de padrões e procedimentos de cibersegurança relevantes para sistemas de TI e TO** (ISO 27001, IEC 64223, etc.) aprovados pela gestão executiva, implantando uma abordagem holística onde TO, IoT, IIoT e segurança de TI são gerenciados por meio de esforço coordenado.

2. **Controlar e minimizar interfaces de rede TO/ICS** com redes externas e terceiros. Monitorar e controlar regularmente as interfaces necessárias.

3. **Nomear pessoal dedicado à cibersegurança** que irá supervisionar a segurança cibernética de TI e TO.

4. **Acelerar a convergência do catálogo de segurança, inventariando todas as soluções de segurança OT/IS IoT usadas na organização** e avaliar a crescente lista de opções autônomas ou multifuncionais, baseadas em plataforma, para a interoperabilidade com as ferramentas de segurança de TI. Segmentar sua rede TO/ICS para diferentes zonas (camada 0,1, etc.) implantando controles de segurança adequados (*firewalls*, diodos unidirecionais de comunicação, VLANs, etc.).

Restringir o acesso aos sistemas em organizações e serviços públicos e privados

1. **Exigir autenticação do usuário e o controle de acesso baseado em função** aos sistemas de processos críticos.

2. **Implementar, monitorar e restringir o acesso remoto** quando exigido por funcionários e terceiros. Limitar o acesso físico de pessoal autorizado às instalações e aos sistemas.

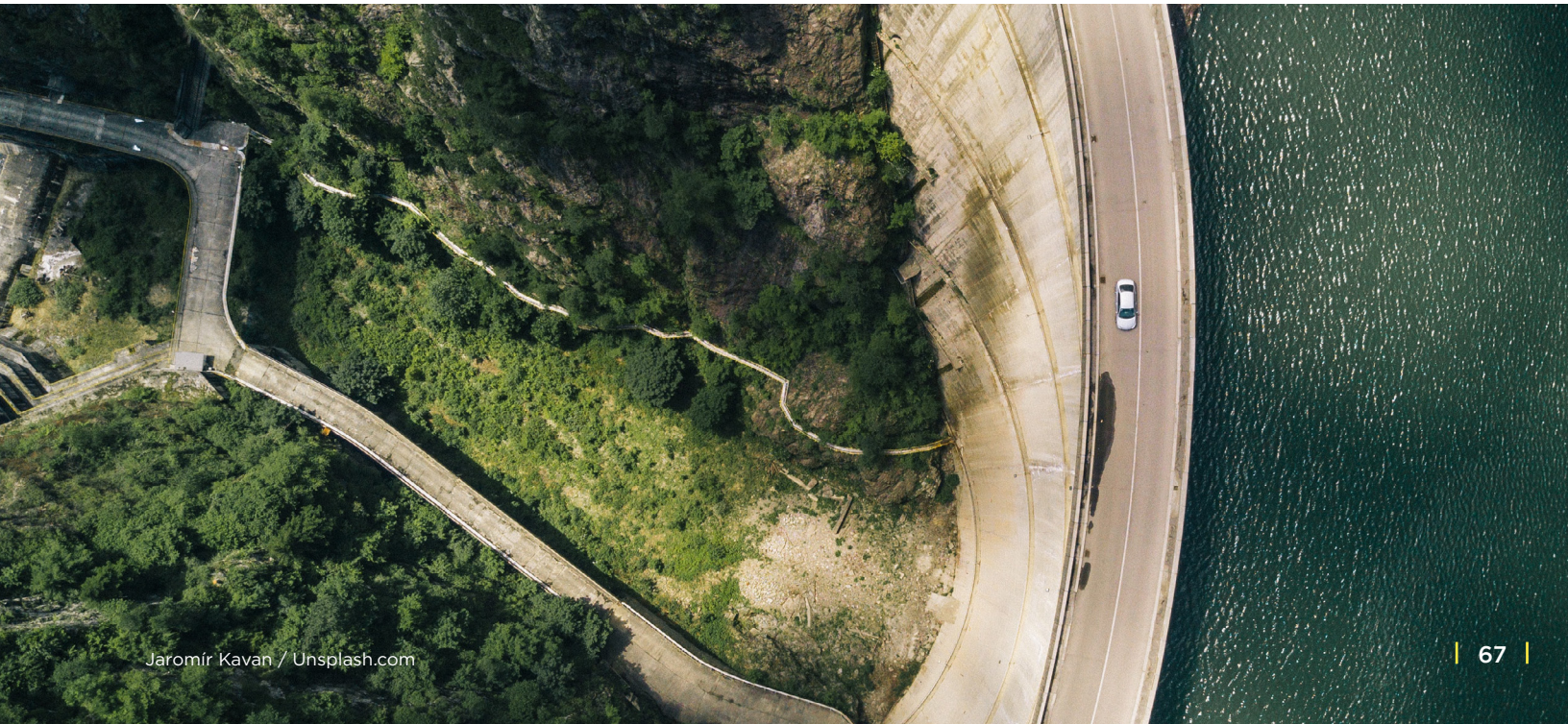
3. **Implantar sistemas de monitoramento cibernético e recursos de detecção de ameaças** (por exemplo, SIEM, IDS, etc.).

Questionário de autoavaliação para avaliar os cenários de cibersegurança em instalações de infraestrutura

No que diz respeito à medição da cibersegurança e à formulação de recomendações específicas para diferentes entidades, o BID implementou uma ferramenta que permitirá que as concessionárias de água e os governos desenvolvam um roteiro de ação. Ele fornece uma visão geral e sugere ações para melhorar o nível de maturidade das organizações, considerando as diferenças entre as situações atuais de cibersegurança e as melhores práticas do setor.

A ferramenta, na forma de um **questionário de autoavaliação, permite que as organizações avaliem sua postura atual de infraestrutura de cibersegurança, revelando as lacunas existentes e fornecendo recomendações** que servem de base para o desenvolvimento de um plano de ação concreto para lidar com ameaças.

Primeiramente, a ferramenta classifica a organização para definir três níveis de risco possíveis (básico, médio e avançado), de acordo com os quais estabelece os requisitos de segurança da informação correspondentes. Em seguida, uma **autoavaliação** é realizada: as perguntas correspondentes ao nível de risco escolhido são apresentadas, e a preparação atual da cibersegurança organizacional é avaliada com base no framework de cibersegurança do Instituto Nacional de Padrões e Tecnologia (NIST, da sigla em inglês). Por fim, a ferramenta calcula uma pontuação com base nas respostas obtidas para cada função e categoria desse framework e fornece recomendações para melhorar o nível de maturidade da organização.



Jaromír Kavan / Unsplash.com

Daniel Morris / Unsplash.com

Bibliografia

Bibliografia

Ablon, L., e A. Bogart. 2017. Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits. RAND Corporation. Disponível em: https://doi.org/10.7249/RR1751.

Aguilar Antonio, J. M. 2021. Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. *Estudios Internacionales*, 53(198): pp. 169–197. January 25, 2021. Disponível em: https://doi.org/10.5354/0719-3769.2021.57067.

Ali, H., e J. Choi. 2019. A Review of Underground Pipeline Leakage and Sinkhole Monitoring Methods Based on Wireless Sensor Networking. MDPI *Sustainability* 11(15), 4007. Disponível em: https://doi.org/10.3390/su11154007.

Aqualia Group. 2019. The New Reality of Water Management: Industry 4.0. Disponível em: https://smartwatermagazine.com/news/aqualia/new-reality-water-management-industry-40.

Aridor-Hershkovitz, R., T. Shwartz Altshuler, e I. Sivan-Sevilla. 2021. What is Cyber Security? Part One: Cyberspace, Cyber Attacks, and Cyber Protection, The Israel Democracy Institute, October, pp. iii-ix. Disponível em: https://www.idi.org.il/media/16859/what-is-cyber-security-part-one-cyberspace-cyber-attacks-and-cyber-protection.pdf.

Belize Crime Observatory. 2020. National Cybersecurity Strategy 2020–2023. Belize: The Ministry of Home Affairs & New Growth Initiatives, November 5, 2020. Disponível em: https://bco.gov.bz/download/national-cybersecurity-strategy-2020-2023/.

Benoliel, D. 2014. Towards a Cyber Security Policy Model: Israel National Cyber Bureau (Incb) Case Study. Global Network of Interdisciplinary Internet & Society Research Centers. Haifa Center of Law and Technology (HCLT). The University of Haifa Faculty of Law, July 2014. Disponível em: https://law.haifa.ac.il/wp-content/uploads/2021/10/TOWARDS-A-CYBER-SECURITY-POLICY-MODEL-ISRAEL-NATIONAL-CYBER-BUREAU-CASE-STUDY-Daniel-Benoliel-reviewed-version.pdf.

Bigelow, S., e B. Lutkevich. 2021. What Is IT/OT Convergence? Everything You Need to Know. In: Search ITOperations. Disponível em: https://www.techtarget.com/searchitoperations/definition/IT-OT-convergence.

Boubaker, KB. 2021. Water Industry: A Look Back at Twenty Years of Cyber Attacks. In Stormshield. Disponível em: https://www.stormshield.com/news/twenty-years-of-cyber-attacks-on-the-world-of-water.

Brangetto, P. e M. Kert-Saint Aubyn. 2015. Economic aspects of national cyber security strategies. NATO Cooperative Cyber Defence Centre of Excellence. Disponível em: https://ccdcoe.org/uploads/2018/10/Economics-of-cybersecurity.pdf.

Calderón, C., e L. Servén. 2020. Infrastructure in Latin America. Office of the Chief Economist, Latin America, and the Caribbean Region, Washington, DC: The World Bank. May 2020, 54.

Canadian Centre for Cyber Security. 2018. An Introduction to the Cyber Threat Environment. Disponível em: https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors.

Caparros, J. 2021. Top Cyber Threats to Latin America and the Caribbean. Mandiant. Disponível em: https://www.mandiant.com/resources/top-cyber-threats-to-latin-america-and-the-caribbean. Acesso: 21 maio 2022.

Check Point Software. s.d. Top 8 Types of Cyber Attacks. Disponível em: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/types-of-cyber-attacks/. Acesso: 21 maio 2022.

Clark, R., S. Panguluri, T. Nelson, e R. Wyman. 2017. Protecting Drinking Water Utilities from Cyberthreats. *Journal of the American Water Works Association* 109. Disponível em: https://doi.org/10.5942/jawwa.2017.109.0021.

Claroty Team82. 2021. Claroty Biannual ICS Risk & Vulnerability Report: 1H 2021. Disponível em: https://claroty.com/wp-content/uploads/2021/08/Claroty_Biannual_ICS_Risk_Vulnerability_Report_1H_2021.pdf.

Computer Security Research Center (CSRC). 2022b. Cyber Attack – Glossary. Disponível em: https://csrc.nist.gov/glossary/term/Cyber_Attack.

_____. 2022a. Cyberspace – Glossary. Disponível em: https://csrc.nist.gov/glossary/term/cyberspace.

Cybersecurity & Infrastructure Security Agency (CISA). 2022. Critical Infrastructure Partnerships and Information Sharing. Disponível em: https://www.cisa.gov/critical-infrastructure-partnerships-and-information-sharing.

_____. 2023. Critical Infrastructure Sectors. Disponível em: https://www.cisa.gov/critical-infrastructure-sectors.

Daigger, G. T., N. Voutchkov, U. Lall e W. Sarni. 2019. The Future of Water: A Collection of Essays on 'Disruptive' Technologies That May Transform the Water Sector in the Next 10 Years. Discussion Paper No. IDB-DP-657. Washington, DC: Inter-American Development Bank (IDB). Disponível em: https://publications.iadb.org/en/future-water-collection-essays-disruptive-technologies-may-transform-water-sector-next-10-years.

Deloitte Insights. 2020. Uncovering the connection between digital maturity and financial performance. Disponível em: https://www2.deloitte.com/content/dam/insights/us/articles/6561_digital-transformation/DI_Digital-transformation.pdf.

Deubelli, T. 2019. Towards Resilient and Sustainable Infrastructure: A Case Study of Governance of Critical Infrastructure Resilience in Costa Rica. Washington, DC: Inter-American Development Bank (IDB). Disponível em: https://publications.iadb.org/en/towards-resilient-and-sustainable-infrastructure-case-study-governance-critical-infrastructure.

European Union Agency for Cybersecurity (ENISA). 2023. Critical infrastructure. Disponível em: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services.

Flashpoint. 2021. From Ransomware to DDoS: Guide to Cyber Threat Actors—How, Why, and Who They Choose to Attack. In: Flashpoint. Disponível em: https://www.flashpoint-intel.com/blog/guide-to-cyber-threat-actors/.

Germano, J. 2019. Cybersecurity Risk & Responsibility in the Water Sector. American Water Works Association. Disponível em: https://www.awwa.org/Portals/0/AWWA/Government/AWWACybersecurityRiskandResponsibility.pdf.

Gillette, J., R. Fisher, J. Peerenboom, e R. Whitfield. 2002. Analyzing Water/Wastewater Infrastructure Interdependencies. Infrastructure Assurance Center, Argonne National Laboratory. Disponível em: https://publications.anl.gov/anlpubs/2002/03/42598.pdf.

Global Cyber Security Capacity Centre. 2021. The Cybersecurity Maturity Model for Nations (CMM). Disponível em: https://gcscc.ox.ac.uk/the-cmm.

Guillaume, F. 2022. The Digital Journey of Water and Sanitation Utilities in Latin America and The Caribbean: What is at Stake and How to Begin. Washington, DC: Inter-American Development Bank (IDB). Disponível em: https://publications.iadb.org/en/digital-journey-water-and-sanitation-utilities-latin-america-and-caribbean-what-stake-and-how-begin.

Hatler, D. 2020. Industry 4.0 & the Water Sector. In: Water Finance & Management. Disponível em: https://waterfm.com/industry-4-0-the-water-sector/.

Hernández, J. 2018. National Cybersecurity Strategies in Latin America. Estrategias Nacionales de Ciberseguridad en América Latina. Digital publication for scientific dissemination on strategic studies, war studies, defense policy and security policies. Global Strategy – University of Granada. Disponível em: https://global-strategy.org/estrategias-nacionales-de-ciberseguridad-en-america-latina/.

HM Government. 2015. National Security Strategy and Strategic Defense and Security Review 2015: Third Annual Report. Crown copyright, Cabinet Office. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819613/NSS_and_SDSR_2015_Third_Annual_Report_-_FINAL__2_.pdf.

_____. 2017. Water Sector Security Strategy. Department for Environmental Food and Rural Affairs. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/602379/water-sector-cyber-security-strategy-170322.pdf.

_____. s.d. Government Cyber Security Strategy: Building a cyber resilient public sector. Crown copyright, Cabinet Office. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1049825/government-cyber-security-strategy.pdf.

_____. 2021. National Cyber Security Centre (NCSC) Annual Review 2021. Disponível em: https://www.ncsc.gov.uk/collection/ncsc-annual-review-2021. Acesso: 9 jul. 2022.

Inter-American Development Bank (IDB), Organization of American States (OAS). 2016. Cybersecurity: Are We Ready in Latin America and the Caribbean? 2016 Cybersecurity Report. Disponível em: https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean. Acesso: 8 jul. 2022.

_____. 2020. 2020 Cybersecurity Report: Risks, Progress, and the Way Forward in Latin America and the Caribbean. Disponível em: https://publications.iadb.org/en/2020-cybersecurity-report-risks-progress-and-the-way-forward-in-latin-america-and-the-caribbean.

IBM Security. 2021. Cost of a Data Breach Report 2021. Disponível em: https://www.ibm.com/downloads/cas/OJDVQGRY.

International Telecommunication Union (ITU). 2019. ICT Facts and Figures. Disponível em: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf.

International Water Association (IWA). 2022. Global Trends & Challenges in Water Science, Research and Management. Disponível em: https://iwa-network.org/publications/global-trends-and-challenges-in-water-science-research-and-management/.

Kaspersky ICS CERT. 2017a. Península Ibérica y Latinoamérica: estadística de las amenazas para sistemas de automatización industrial, primer semestre de 2017. In: SecureList by Kaspersky. Disponível em: https://securelist.lat/threat-landscape-for-industrial-automation-systems-in-h1-2017/85531/.

Kaspersky. 2017b. The Human Factor in IT Security: How Employees Are Making Businesses Vulnerable from Within. In: Kaspersky Daily. Disponível em: https://www.kaspersky.com/blog/the-human-factor-in-it-security/. Acesso: 26 set. 2022.

Lavinder, K. 2016. Cyberattacks: Is Latin America Prepared? Disponível em: https://www.airuniversity.af.edu/Portals/10/ASPJ_Spanish/Journals/Volume-28_Issue-4/2016_4_05_lavinder_s_eng.pdf.

Lewis, J. 2018. Economic Impact of Cybercrime-No Slowing Down Report. McAfee and the Center for Strategic and International Studies (CSIS). Disponível em: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf.

_____. 2020. The hidden cost of Cybercrime. McAfee and the Center for Strategic and International Studies (CSIS). Disponível em: https://companies.mybroadband.co.za/axiz/files/2021/02/eBook-Axiz-McAfee-hidden-costs-of-cybercrime.pdf.

Menashri, H., e G. Baram. 2015. Critical Infrastructures and Their Interdependence in a Cyber Attack – The Case of the U.S. *Military and Strategic Affairs* 7(1). Disponível em: https://www.inss.org.il/wp-content/uploads/systemfiles/5_Menashri_Baram.pdf.

Mirjana, S., A. Hasanbeigi, N. Neftenov, and Tambourine Innovation Ventures. 2020. Use of 4IR Technologies in Water and Sanitation in Latin America and the Caribbean. Technical Note No. IDB-TN-1910. Washington, DC: Inter-American Development Bank (IDB). Disponível em: https://publications.iadb.org/en/use-of-4ir-technologies-in-water-and-sanitation-in-latin-america-and-the-caribbean.

Mission of Israel to the UN in Geneva. 2021. Water and Cyber Security – Part II. Disponível em: https://embassies.gov.il/UnGeneva/NewsAndEvents/Events/Pages/20210413-Water-and-Cyber-Security-Part-II.aspx.

Moore, S. 2021b. Gartner Predicts 30% of Critical Infrastructure Organizations Will Experience a Security Breach by 2025. Disponível em: https://www.gartner.com/en/newsroom/press-releases/2021-12-2-gartner-predicts-30--of-critical-infrastructure-organi.

_____. 2021a. Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans. Disponível em: https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we.

Murray, G., M. Johnstone, e C. Valli. 2017. The Convergence of IT and OT in Critical Infrastructure. *In: The Proceedings of the 15th Australian Information Security Management*

Conference, Edith Cowan University, Perth, Western Australia, 5-6 December 2017, p. 149-155. Disponível em: **https://doi.org/10.4225/75/5A84F7B595B4E**.

Organization of American States (OAS). 2018. Critical Infrastructure Protection in Latin America and the Caribbean 2018. Disponível em: **https://www.oas.org/es/sms/cicte/cipreport.pdf**.

_____. 2020. Cybersecurity Capacity Review Brazil 2020. Global Cyber Security Capacity Centre, Department of Computer Science, University of Oxford. Disponível em: **https://www.oas.org/en/sms/cicte/docs/ENG-CYBERSECURITY-CAPACITY-REVIEW-BRAZIL.pdf**.

Organization for Economic Co-operation and Development (OECD) Water. s.d. Infographic – What Are the Impacts of Water Pollution? Disponível em: **https://www.oecd.org/fr/sites/oecdwater/infographic-impacts-of-water-pollution.htm**.

Pimenta Klein, B., e Y. Boguslavskiy. 2020. Latin America Threat Landscape: The Paradox of Interconnectivity. AdvIntel. Disponível em: **https://web.archive.org/web/20230126221027/https://www.advintel.io/post/latin-america-threat-landscape-the-paradox-of-interconnectivity**.

Prado, P. 2011. The Impact of the Internet in Six Latin American Countries. Western Hemisphere Security Analysis Center. Disponível em: **https://digitalcommons.fiu.edu/whemsac/6/**.

Privacy International. 2019. State of Privacy Argentina. January 23, 2019. Disponível em: **https://privacyinternational.org/state-privacy/57/state-privacy-argentina**.

Pursiainen, C., P. Lindblom, P. Francke, e Nordregio. 2007. Towards a Baltic Sea Region Strategy in Critical Infrastructure Protection. Stockholm: Nordregio. Disponível em: **https://www.diva-portal.org/smash/get/diva2:700420/FULLTEXT01.pdf**.

Rinaldi, S.M., J. Peerenboom, e T. Kelly. 2001. Identifying, Understanding and Analyzing. In Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine,* 21(6): 11–25. Doi: 10.1109/37.969131.

Saavedra, B. 2015. Cybersecurity in Latin America and The Caribbean: The State of Readiness for the Defense of Cyberspace. Washington, DC: William J. Perry, Center for Hemispheric Defense Studies. Disponível em: **https://bco.wimp.bz/file_directory/files/cybersecurity/20150730LatinAmericaCaribbeanCybersecurityStateofReadiness.pdf**.

Siboni, G., D. Cohen, e A. Rotbart. 2013. The Threat of Terrorist Organizations in Cyberspace. *Military and Strategic Affairs,* 5(3).

Snow, R. 2022. 3 Planning Assumptions for Securing Cyber-Physical Systems of Critical Infrastructure. Gartner Research. Disponível em: **https://www.gartner.com/en/articles/3-planning-assumptions-for-securing-cyber-physical-systems-of-critical-infrastructure**.

Srivastava, M. 2020. Israel-Iran Attacks: 'Cyber Winter Is Coming.' *Financial Times,* 31 May 2020. Disponível em: **https://www.ft.com/content/3ea57426-40e2-42da-9e2c-97b0e39dd967**.

Stankovic, M., A. Hasanbeigi, e N. Neftenov. 2020. Use of 4RI technologies in water and sanitation in Latin America and the Caribbean. Washington, DC: Inter-American Development Bank (IDB). Disponível em: **https://publications.iadb.org/en/use-of-4ir-technologies-in-water-and-sanitation-in-latin-america-and-the-caribbean**.

Stouffer, K., V. Pillitteri, S. Lightman, M. Abrams, e A. Hahn. 2015. Guide to Industrial Control Systems (ICS) Security. National Institute of Standards and Technology (NIST), U.S. Department of Commerce. Disponível em: **https://doi.org/10.6028/NIST.SP.800-82r2**.

Tabansky, L. 2011. Critical Infrastructure Protection against Cyber Threats. *Military and Strategic Affairs,* 3(2) November 2011. Disponível em: **https://www.inss.org.il/wp-content/uploads/2017/02/FILE1326273687-1.pdf**.

Thielemann, K., W. Voster, B. Pace, R. Contu, and R. Hunter. 2021. Predicts 2022: Cyber-Physical Systems Security — Critical Infrastructure in Focus. Gartner Research, November 17, 2021. Disponível em: **https://www.gartner.com/en/documents/4008351**.

US Water Sector Coordinating Council. 2021. Water and Wastewater Systems, Cybersecurity 2021, State of the Sector. Disponível em: **https://www.waterisac.org/system/files/articles/FINAL_2021_WaterSectorCoordinatingCouncil_Cybersecurity_State_of_the_Industry-17-JUN-2021.pdf**.

Van Raemdonck, N. 2020. Cyber Diplomacy in Latin America. In: EU Cyber Direct, EU Institute for Security Studies. Disponível em: **https://eucyberdirect.eu/research/cyber-diplomacy-in-latin-america**.

Water Information Sharing and Analysis Center (WaterISAC). 2021. WaterISAC 2021 Survey. Disponível em: **https://www.waterisac.org/2021survey**.

Weiss, J. 2008. Assuring Industrial Control System (ICS) Cyber Security. Applied Control Solutions, LLC, p. 14.

Wesley, C. 2023. What is the CIA Triad? Definition, Explanation and Examples. WhatIs.com. Disponível em: **https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA**.

Williamson, Graham. 2015. OT, ICS, SCADA – What's the Difference? In: KuppingerCole Analysts. Disponível em: **https://www.kuppingercole.com/blog/williamson/ot-ics-scada-whats-the-difference**. Acesso: 21 maio 2022.

World Health Organization (WHO). 2019. Water, Sanitation, and Hygiene in Health Care Facilities. Seventy-Second World Health Assembly Agenda item 12.5. Disponível em: **https://apps.who.int/iris/bitstream/handle/10665/329290/A72_R7-en.pdf?sequence=1&isAllowed=y**.

Ivan Bandura / Unsplash.com

Dan Meyers / Unsplash.com

Apêndices

Apêndice A

Questionário de entrevista para empresas de serviços públicos

1. Como você descreveria sua organização?

2. Qual é o tamanho da sua organização em termos de:

i. número de instalações;

ii. número de funcionários;

iii. nível de produção;

iv. faturamento anual.

3. A organização é reconhecida como IC? Como infraestrutura essencial? Nenhuma das duas?

4. Quem é a autoridade reguladora?

5. Quantas pessoas trabalham no departamento de TI? E com cibersegurança?

6. Existe o cargo de diretor de cibersegurança na sua organização?

7. Qual é o orçamento aproximado (em %) do departamento de TI? E do departamento cibernético?

8. A ameaça cibernética é reconhecida como um risco?

9. Existem regulamentos, diretrizes ou requisitos de cibersegurança provenientes do Estado?

10. Você tem conhecimento de algum programa de cibersegurança para o setor no nível de política ou regulatório? Descreva.

11. Existem requisitos internos de cibersegurança?

12. O setor de A&S é reconhecido como IC?

13. Você já sofreu um ciberataque ou passou por um ciberevento? Ou um evento operacional/de manutenção inexplicável?

14. Com que frequência você revisa os controles e procedimentos de cibersegurança?

15. Você tem um plano anual de cibersegurança? Em caso afirmativo, o que ele inclui (ou seja, treinamento, *hacking* ético, atualização de inventário de dispositivos, etc.)?

16. Qual é o dano potencial de um evento cibernético (não um ataque)? (Financeiro, ambiental, de segurança pública ou com outras consequências).

17. Quando foi a última auditoria cibernética? Existem atividades pendentes?

18. Existe um programa de treinamento em cibersegurança para funcionários?

19. A empresa usa métodos de acesso remoto seguro?

20. Como você descreveria os riscos cibernéticos atuais e futuros enfrentados pelo setor de A&S na ALC?

21. Como você avaliaria o nível de preparação do seu sistema para ataques cibernéticos contra IC e, especificamente, no setor de A&S? Como você avaliaria o nível de preparação da organização?

22. Até onde você sabe, qual país da região da ALC tem as capacidades mais robustas de gestão de defesa cibernética do setor de A&S?

23. Existem ferramentas de cibersegurança desenvolvidas para outros setores (por exemplo, rede elétrica, oleodutos/gasodutos) que sua concessionária adaptou para uso no setor de A&S?

24. Se um ator de ameaças comprometesse o ativo da organização, quais seriam os piores cenários realistas?

25. Quais interconexões são necessárias para que os sistemas funcionem?

26. A organização desenvolveu e praticou procedimentos de resposta a incidentes que combinam processos de resposta de TI e TO?

Apêndice B

Questionário de entrevista para reguladores e órgãos federais

1. Como você descreveria a organização?
2. Qual é o tamanho e os recursos da unidade cibernética que supervisiona o setor de A&S?
3. Como você descreveria os riscos cibernéticos atuais e futuros enfrentados pelo setor de A&S na ALC?
4. A ameaça cibernética é reconhecida como um risco?
5. Como você avaliaria o nível de preparação do seu país para ciberataques contra IC e, especificamente, o setor de A&S?
6. Como você descreveria os riscos cibernéticos atuais e futuros enfrentados pelo setor de A&S na ALC?
7. Existem regulamentos, diretrizes ou requisitos de cibersegurança estabelecidos pelo governo federal?
8. Você tem conhecimento de algum programa de cibersegurança para o setor no nível de política ou regulatório? Descreva.
9. Até onde você sabe, qual país da região da ALC tem as capacidades mais robustas de gestão de defesa cibernética do setor de A&S?
10. O setor de A&S é reconhecido como IC?
11. A sua organização sofreu (ou gerenciou) um ciberevento/ciberataque?
12. Com que frequência os procedimentos e requisitos de cibersegurança são revisados?
13. Existe um plano anual de cibersegurança na organização? Em caso afirmativo, o que ele inclui (ou seja, treinamento, conscientização, exercício nacional, etc.)?
14. Qual é o dano potencial de um ciberevento no setor de A&S (não necessariamente um ataque)? (Financeiro, ambiental, de segurança pública ou com outras consequências)
15. Existem ferramentas de cibersegurança desenvolvidas para outros setores (por exemplo, rede elétrica, oleodutos/gasodutos) que a sua organização adaptou para uso no setor de A&S?

BID

BID | LAB