adelat

www.adelat.com

REDES SOB ATAQUE

CIBERSEGURANÇA ELÉTRICA NA ERA DA TRANSIÇÃO ENERGÉTICA



DSO Review n.º 11 · Série: Tecnologia e Operação

AUTORES

Alessandra Amaral, Roberto Cajamarca Gómez, Nivia Celestino, Joaquín Lazo Sánchez.

COLABORADORES

Daniel Aranibar, Edward Kenneth Arias Palacio, Rafael Bacis, Guillermo Andrés Cepeda Rodríguez, Nicolás Elgueta C., Alfredo Gallegos González, Jorge Gelmetti, Cristóbal Jaramillo, Luis Jorge Llapiz, Mario Alberto Martínez Martínez, Rubens Mazzon Jr., Gerald Moran, Rodrigo Oliva, Luis Quispe, Emanuel Rodríguez, Rosimiro Santos Ferreira, Juanjo Servetti, Franchesco Somontes Marín, Mariela Uribe Olivas, Fernando Varela, Julián David Velasco Jaramillo, Iván Zamudio.

PALAVRAS-CHAVE

Cibersegurança; distribuição elétrica; América Latina; transição energética; infraestrutura crítica; tecnologias de operação (OT); maturidade em cibersegurança; regulação de cibersegurança; reconhecimento tarifário; ciber-resiliência.

© 2026 Associação de Distribuidores de Eletricidade da América Latina (ADELAT). Todos os direitos reservados. Autoriza-se a reprodução total ou parcial para fins não comerciais, desde que citada a fonte.

Agosto de 2026

1. INTRODUÇÃO 4

2. O RISCO CIBERNÉTICO NOS SISTEMAS DE DISTRIBUIÇÃO 6

3. DIMENSÕES DA CIBERSEGURANÇA E SITUAÇÃO ATUAL DO SETOR 9

3.1. Segurança da infraestrutura de operação 9
3.2. Capacidade de detecção e resposta 11
3.3. Terceiros, serviços em nuvem e proteção de dados 13
3.4. Cultura organizacional e talentos especializados 14
3.5. Governança, orçamento e papel do conselho 14

4. A RESPOSTA REGULATÓRIA NA AMÉRICA LATINA 17

4.1. O Contexto 17

5. ABORDAGENS REGULATÓRIAS INTERNACIONAIS E MELHORES PRÁTICAS 23

5.1. Estados Unidos: obrigatoriedade federal para o sistema atacadista, voluntariedade estadual para a distribuição 24
5.2. União Europeia: da norma horizontal ao código de rede setorial 26
5.3. Reino Unido: o regulador de energia como autoridade de cibersegurança 28
5.4. Austrália: a proporcionalidade como princípio de design 29
5.5. Ontário: regulação de maturidade para distribuidoras heterogêneas 31
5.6. Índia: regulação em um sistema de grande escala e maturidade desigual 31
5.7. Mecanismos que a experiência internacional coloca sobre a mesa 32
5.8. Leituras para a América Latina 35

6. CONCLUSÕES E RECOMENDAÇÕES REGULATÓRIAS 37

7. REFERÊNCIAS 40

01
INTRODUÇÃO

A transição energética tornou-se uma das transformações com maior respaldo de nosso tempo, exigida pela sociedade, assumida pelos governos e em curso em todo o mundo impulsionada pela tecnologia. Seu propósito é descarbonizar a economia fazendo da eletricidade limpa o principal vetor energético, materializando-se em redes com medição inteligente, telecontrole e automação da operação, na geração distribuída e na crescente eletrificação do transporte e dos usos finais de energia. A América Latina não é exceção, seus planos energéticos e agendas regulatórias já comprometem boa parte dessa modernização, em um cenário no qual a necessidade de digitalizar a rede é cada vez mais relevante.

Essa digitalização, embora necessária e habilitante, traz uma consequência menos visível. Ao incorporar inteligência e conectividade, a rede também acumula exposição, pois todo dispositivo digital pode ser acessado remotamente por terceiros não autorizados para extrair informações, alterar seu funcionamento ou deixá-lo fora de serviço. Cada novo medidor inteligente, inversor conectado ou equipamento tele controlado que entra em operação representa, ao mesmo tempo, um novo ponto de entrada para a infraestrutura de que depende o fornecimento. A superfície de ataque da rede cresce, portanto, no mesmo ritmo da própria transição.

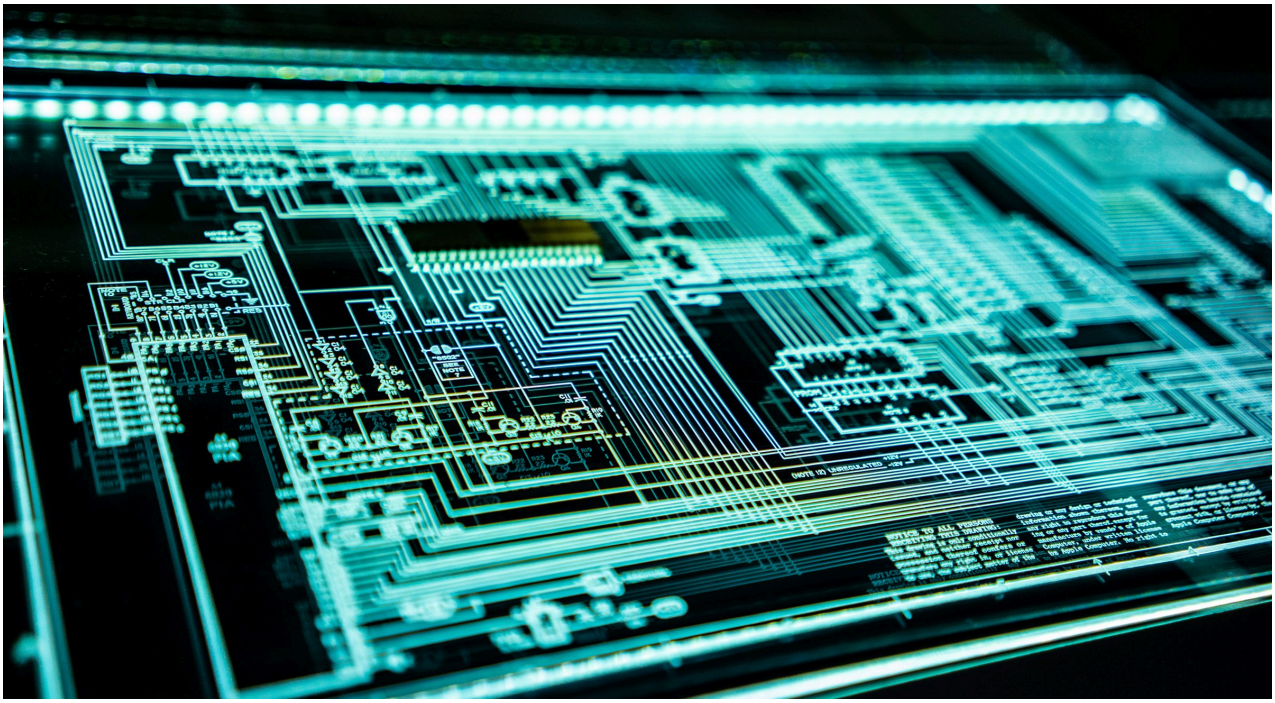
A gravidade dessa exposição não reside na falha informática em si, mas no fato de que suas consequências se transferem diretamente para a vida dos consumidores. Para quem fica sem eletricidade, pouco importa se a interrupção foi causada por uma tempestade ou por uma invasão cibernética, porque o efeito é o mesmo: o comércio paralisado, os domicílios sem luz e os serviços essenciais operando com suprimentos de emergência. A regulação tampouco distingue entre uma origem e outra, pois essa interrupção fica registrada nos mesmos indicadores de continuidade que são exigidos e sancionados. O que muda é a causa e o que é preciso fazer para evitá-la, porque um ataque não depende das condições climáticas, pode se repetir, escolhendo o momento de maior dano e nenhuma das medidas reconhecidas e remuneradas pela regulação hoje, desde a poda preventiva até o reforço das redes, é capaz de preveni-lo. À interrupção do fornecimento somam-se outros danos que a rede tradicional não poderia provocar, como o vazamento dos dados de consumo de milhões de consumidores, que revelam rotinas e presença nos domicílios e não se resolvem com a recomposição do serviço ou a degradação física dos equipamentos por quem consegue controlá-los à distância. Um ciberataque bem-sucedido contra uma distribuidora, portanto, não é vivenciado como um incidente informático, mas como uma agressão à infraestrutura crítica de que depende a vida cotidiana de um território inteiro.

O diagnóstico a seguir baseia-se em evidências primárias coletadas junto às próprias empresas distribuidoras. No âmbito do seu Programa de Benchmarking, a ADELAT desenvolveu um exercício dedicado à maturidade em cibersegurança, com a participação de distribuidoras de toda a América Latina e de escalas muito distintas, desde cooperativas rurais até grandes grupos com milhões de consumidores. Seus resultados descrevem um setor em movimento, no qual um grupo de empresas já alcançou níveis elevados de maturidade enquanto outra parcela significativa ainda está desenvolvendo capacidades básicas. O achado mais relevante, contudo, não é o nível médio, mas sua distribuição interna, dado que os maiores avanços se verificam

na separação entre as redes corporativa e de operação, âmbito em que o setor historicamente concentrou seus investimentos. As lacunas mais profundas estão nos dispositivos de campo, que são justamente os que a transição energética multiplica. A exposição cresce, portanto, com maior velocidade onde a capacidade de contê-la é mais frágil.

A origem dessa disparidade não se encontra, principalmente, na vontade das empresas, mas no marco que orienta suas decisões de investimento. Na maioria dos países da região, a cibersegurança não está definida como uma obrigação setorial com padrões próprios e verificáveis e, onde já existe legislação geral sobre o tema, sua aplicação ao segmento de distribuição ainda não se traduz em requisitos operacionais nem no reconhecimento de seus custos. Cada distribuidora precisa então financiar sua proteção deslocando recursos de rubricas que já são reconhecidas, de modo que o nível de segurança termina dependendo da convicção e da folga financeira de cada empresa, o que explica a dispersão revelada pelo benchmarking. A essa indefinição soma-se uma dificuldade de design mais profunda, pois proteger uma rede digitalizada não é um investimento que se executa uma vez, mas uma capacidade que precisa ser sustentada ao longo do tempo, enquanto os marcos tarifários foram construídos para reconhecer ativos físicos e não capacidades operacionais contínuas. O resultado é um descompasso produzido pela própria regulação, que impulsiona a digitalização da rede por um lado e omite, pelo outro, as condições para protegê-la. Corrigir esse descompasso implica definir a exigência, graduá-la conforme o porte e a criticidade de cada empresa e reconhecer seu custo dentro das receitas reguladas, três decisões que outras jurisdições já tomaram e que na América Latina ainda estão pendentes.

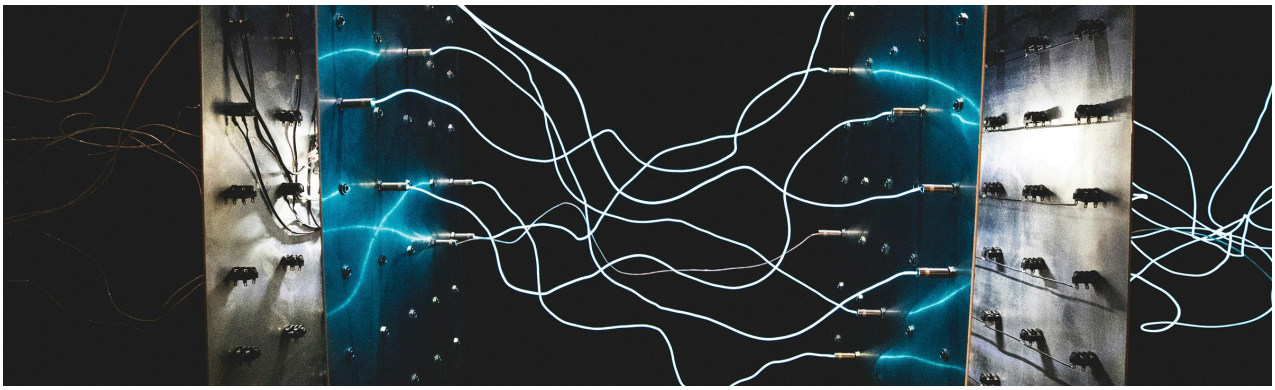
O documento está estruturado da seguinte forma. O Capítulo 2 caracteriza o risco cibernético próprio das redes de distribuição e o que o distingue da segurança informática corporativa. O Capítulo 3 organiza as dimensões que compõem a maturidade nessa área e apresenta o que o benchmarking revela em cada uma delas. O Capítulo 4 examina o estado da regulação na América Latina e o alcance das exigências vigentes. O Capítulo 5 revisa a experiência de jurisdições que já enfrentaram esse problema e extrai os critérios de design aplicáveis à região. O Capítulo 6 sintetiza o panorama regional e formula recomendações dirigidas aos reguladores.



02

O RISCO CIBERNÉTICO NOS SISTEMAS DE DISTRIBUIÇÃO

A cibersegurança de uma rede de distribuição não equivale à de um escritório. Em toda distribuidora coexistem dois mundos digitais: o dos sistemas corporativos que gerenciam o faturamento e as informações comerciais e o dos sistemas de operação que supervisionam e comandam a rede física[1]. Proteger o segundo é um problema de natureza distinta, porque seus ativos estão dispersos por milhares de quilômetros sem vigilância permanente, boa parte dos equipamentos foi projetada antes da conectividade e opera com vida útil de vinte anos ou mais, sem admitir atualização, tudo ocorre em tempo real, de modo que parar um sistema para revisá-lo já constitui o dano que se quer evitar. A prioridade também se inverte, pois no ambiente corporativo protege-se antes de tudo a confidencialidade das informações, enquanto na operação protegem-se a disponibilidade e a integridade do controle, razão pela qual as práticas habituais de segurança informática são insuficientes. Essa distância entre o perímetro corporativo e a operação é também o que gradua a gravidade de um incidente, porque o decisivo não é que um ataque ocorra, mas até onde ele consegue chegar.



Os ataques já documentados contra empresas elétricas podem ser ordenados por esse critério. No primeiro nível, o ataque não alcança a rede. O ransomware[2] entra pelos sistemas corporativos e deixa fora de operação o faturamento, o portal virtual e o atendimento ao consumidor durante dias, enquanto o fornecimento continua sem alteração. Nesse mesmo nível situam-se os vazamentos de informações comerciais, um dos quais, ocorrido na região, colocou em circulação mais de catorze milhões de registros de consumidores com endereço e número de medidor, segundo relatos da imprensa que a empresa afetada nunca confirmou (Adaptix Networks, 2022). Isso costuma ser lido como uma crise administrativa, mas nem sempre fica nesse patamar, porque quando a empresa não consegue determinar até onde chegou o intruso, recorre ao desligamento preventivo da operação,

[1] A indústria denomina ambientes de TI os sistemas de informação corporativos e ambientes de TO (tecnologia de operação) os que supervisionam e controlam processos físicos.

[2] Programa malicioso que cifra as informações de uma organização e as mantém inutilizáveis até o pagamento de um resgate em troca da chave que as decifra.

como ocorreu em 2023 na Dinamarca, onde vinte e duas empresas de energia foram comprometidas por meio de uma vulnerabilidade no equipamento de um fornecedor e várias optaram por se desconectar das redes de dados (SektorCERT, 2023). A situação está longe de ser excepcional, pois três em cada quatro incidentes de ransomware atendidos em ambientes industriais acabam degradando a operação e um em cada quatro a interrompe completamente (Dragos, 2025). Interromper o serviço, portanto, não exige alcançar os sistemas de controle.

O nível seguinte alcança os sistemas de controle e, nesse ponto, o incidente deixa de ser um problema da empresa e se transforma em uma interrupção do fornecimento. Em dezembro de 2015, os atacantes assumiram o comando de três distribuidoras ucranianas e abriram os disjuntores remotamente, como faria um operador, deixando duzentos e vinte e cinco mil consumidores sem eletricidade, enquanto um ataque paralelo saturava a central telefônica para impedir que esses mesmos consumidores reportassem a falha. A recomposição exigiu o envio de equipes para operar manualmente as subestações, porque o controle remoto havia deixado de responder e vários equipamentos de comunicação ficaram inoperantes após o apagamento de seu firmware[3] (Lee et al., 2016). Um ano depois, o malware[4] industrial conhecido como Industroyer dispensou o operador humano e se comunicou diretamente com os protocolos das subestações para deixar parte de Kiev sem eletricidade por cerca de uma hora (Cherepanov, 2017). Em 2022, uma versão atualizada desse mesmo programa foi detectada e neutralizada horas antes de ser executada (CERT-UA, 2022; ESET Research, 2022). A capacidade existe, está comprovada em campo e continua sendo aperfeiçoada.



Fig. 1. Os dois níveis de um ciberataque contra uma distribuidora

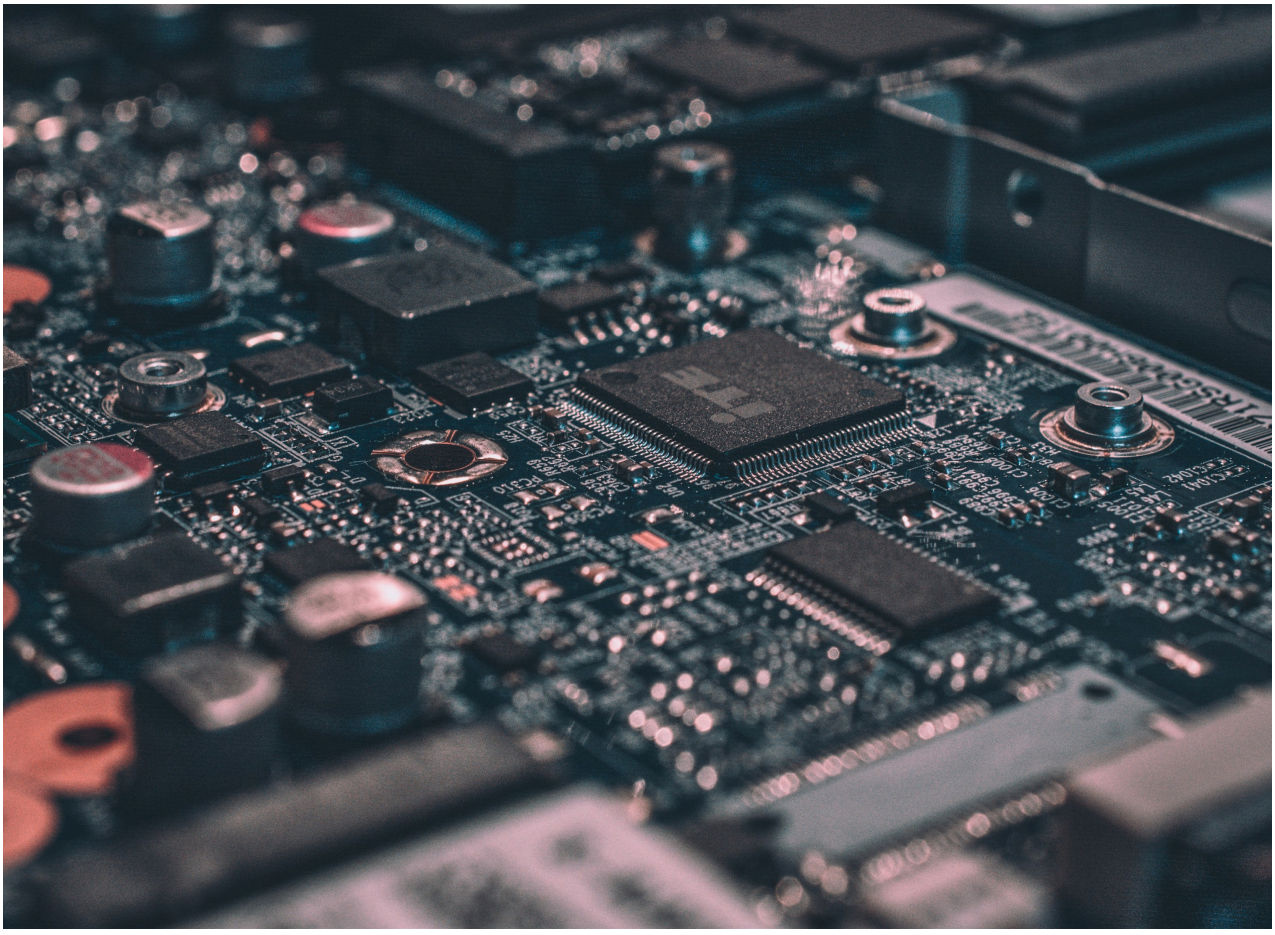
O fato de que o registro regional se concentre no primeiro nível não autoriza concluir que o segundo esteja fora de alcance, porque até pouco tempo atrás a América

[3] Programa gravado na memória do próprio equipamento, que governa seu funcionamento básico. Diferentemente de um aplicativo, não pode ser desinstalado nem reinstalado à distância com facilidade: recuperá-lo costuma exigir intervenção física no dispositivo.

[4] Termo que designa qualquer programa projetado para danificar um sistema, alterar seu funcionamento ou obter acesso não autorizado a ele. O ransomware é uma de suas variantes.

Latina não tinha obrigação de notificar incidentes e, onde essa obrigação surgiu, foi após a ocorrência de um ataque naquele mesmo país, de modo que o mapa disponível descreve melhor o estado da norma do que o da ameaça. Tampouco existe, nos incidentes ocorridos na região, investigação independente que tenha estabelecido se a operação permaneceu intacta por design ou porque o atacante não estava preparado para cruzar essa barreira. O rigor também obriga à advertência inversa, pois episódios atribuídos pela imprensa a ciberataques resultaram ser falhas operacionais, como o apagão que afetou Argentina e Uruguai em 2019 (La Tercera, 2019). O que admite mensuração é a capacidade de cada empresa de conter um ataque antes que ele alcance a operação, sendo a isso que se dedica o Capítulo 3.

> A capacidade existe, está comprovada em campo e continua sendo aperfeiçoada.



03

DIMENSÕES DA CIBERSEGURANÇA E SITUAÇÃO ATUAL DO SETOR

A segurança de uma distribuidora não se resolve em um único plano nem se degrada de maneira uniforme, de modo que um diagnóstico útil para o regulador exige antes um vocabulário comum. Este capítulo o constrói a partir de cinco dimensões que organizam o problema: desde a proteção da infraestrutura que opera a rede até a governança que decide e financia essa proteção, passando pela capacidade de detectar e responder, pela exposição introduzida por terceiros e pelo tratamento de dados dos usuários e pelas pessoas que sustentam tudo isso. Cada dimensão é explicada primeiro em seus próprios termos e ilustrada depois com os autorrelatos que vinte e cinco distribuidoras de dez países da América Latina entregaram ao Programa de Benchmarking da ADELAT, refletindo, portanto, a posição que cada empresa se atribui antes de uma verificação externa de seus controles. Como o objetivo deste diagnóstico é estabelecer onde o setor avançou, onde não avançou e o que disso depende de decisões que a própria empresa não controla, todas as informações são apresentadas de forma anônima e agregada.

3.1. SEGURANÇA DA INFRAESTRUTURA DE OPERAÇÃO

A rede de distribuição deixou de ser um sistema exclusivamente físico quando a operação passou a ser exercida à distância. Hoje uma subestação abre ou fecha um disjuntor porque recebe uma instrução que trafega por uma rede de dados e essa instrução não distingue se foi enviada por um operador ou por alguém que conseguiu ocupar seu lugar. Essa é a camada que o Capítulo 2 identificou como fronteira decisiva, porque antes dela a empresa ainda decide se interrompe o serviço e depois dela quem decide é o atacante. Sua proteção foi organizada durante décadas em torno de um anel: a separação entre a rede de operação e a rede corporativa. O diagnóstico regional perguntou sobre esse anel, sobre os canais que precisam atravessá-lo para que a operação possa ser exercida à distância e sobre os dispositivos instalados no campo, que pertencem à rede de operação mas estão onde nenhum perímetro alcança. As três respostas descrevem um declínio à medida que a proteção se afasta do centro de controle, seguindo a mesma ordem em que a modernização da rede foi empurrando a operação para fora.

O anel separa duas redes que a empresa precisa manter distintas. Pela rede corporativa, que deve estar aberta à internet e a centenas de usuários, circulam o correio eletrônico, o faturamento e os sistemas de gestão. Pela rede de operação trafegam as ordens que comandam os disjuntores. Quando ambas formam uma única rede, quem abriu um arquivo infectado em um computador de escritório fica conectado ao sistema de controle sem nenhuma barreira intermediária, a segregação consiste em interpor essa barreira. Catorze das 23 empresas que responderam a implantaram com firewalls industriais e uma zona intermediária, de modo que tudo que cruza passa por um equipamento capaz de interpretar os protocolos elétricos e distinguir uma instrução legítima de uma ilegítima, outras três mantêm a rede de operação isolada, com dados que saem mas nunca entram. As seis restantes se apoiam na configuração de equipamentos de rede compartilhados ou, em dois casos, não têm nenhum perímetro definido.

O anel não pode ser contínuo, porque a operação à distância exige canais que o atravessem. Uma subestação sem pessoal permanente precisa ser atendida de outro lugar, de modo que esses canais existem por design e não por descuido, o acesso remoto é o que torna operável uma rede extensa. A questão, portanto, não é se esses canais existem, mas quem entra por eles e com que registro. O erro mais frequente é tratar a VPN[5] como solução, porque ela cifra o que trafega, mas não verifica quem está do outro lado, uma credencial roubada entra por esse mesmo túnel sem levantar suspeitas. Doze empresas já exigem um segundo fator de autenticação, que resolve a entrada mas não o que ocorre depois. O ponto ideal é que a permissão seja criada para uma tarefa específica, expire quando a tarefa termina e fique registrada, de modo que, entre um trabalho e o seguinte, não exista nenhum acesso permanente passível de roubo, apenas uma das vinte empresas que responderam chegou a esse nível.

Os dispositivos de campo são, na prática, canais permanentes. Um medidor inteligente ou um religador mantém comunicação constante com os sistemas centrais para reportar medições e receber ordens, de modo que cada equipamento instalado é uma conexão que não se abre para uma tarefa e depois se fecha, mas que dura tanto quanto o equipamento durar no poste. E não se trata de poucas aberturas vigiadas, mas de milhares ou milhões de pontos em postes e caixas de rua, fora do alcance de qualquer perímetro. Do outro lado também não há uma pessoa à qual retirar permissões, mas um equipamento cuja identidade veio de fábrica e costuma ser a mesma para toda a frota, de modo que basta retirar um do poste para ter a identidade de todos. Boa parte foi instalada para durar vinte ou trinta anos e não admite correções, motivo pelo qual as empresas os gerenciam por contenção antes que por atualização, como descrevem as respostas abertas em toda a região. O ideal é que cada dispositivo tenha identidade própria e comunicações cifradas, apenas uma das 19 empresas que responderam declara ter alcançado esse nível, enquanto cinco mantêm as credenciais que vêm de fábrica.

Ordenados por desempenho, as três frentes ficam também ordenadas pela natureza de seu custo. O anel, que se constrói uma vez e pode ser dado por concluído, é a frente mais bem resolvida, com 74% das empresas em nível avançado. Os canais, cujos controles se implantam uma vez, mas que só protegem se alguém administrar cada inclusão, cada exclusão e cada permissão todos os dias, recuam para 65%. Os dispositivos de campo, cujo custo não depende de quantas pessoas há para administrar, mas de quantos equipamentos estão instalados e que cresce a cada programa de medição inteligente, caem para 21%. O desempenho do setor diminui à medida que o custo deixa de se parecer com um investimento e começa a se parecer com um gasto operacional permanente. Essa correlação aponta para os esquemas de remuneração, porque os marcos tarifários reconhecem com relativa facilidade o investimento que entra na base de ativos e tratam o gasto recorrente como um custo a comprimir em nome da eficiência, de modo que a parte da cibersegurança mais necessária é também a que o modelo regulatório menos sabe remunerar.

[5] VPN: Rede Privada Virtual, pela sigla em inglês. Canal cifrado que protege as informações enquanto trafegam por uma rede pública, mas que por si só não confirma a identidade de quem o utiliza.

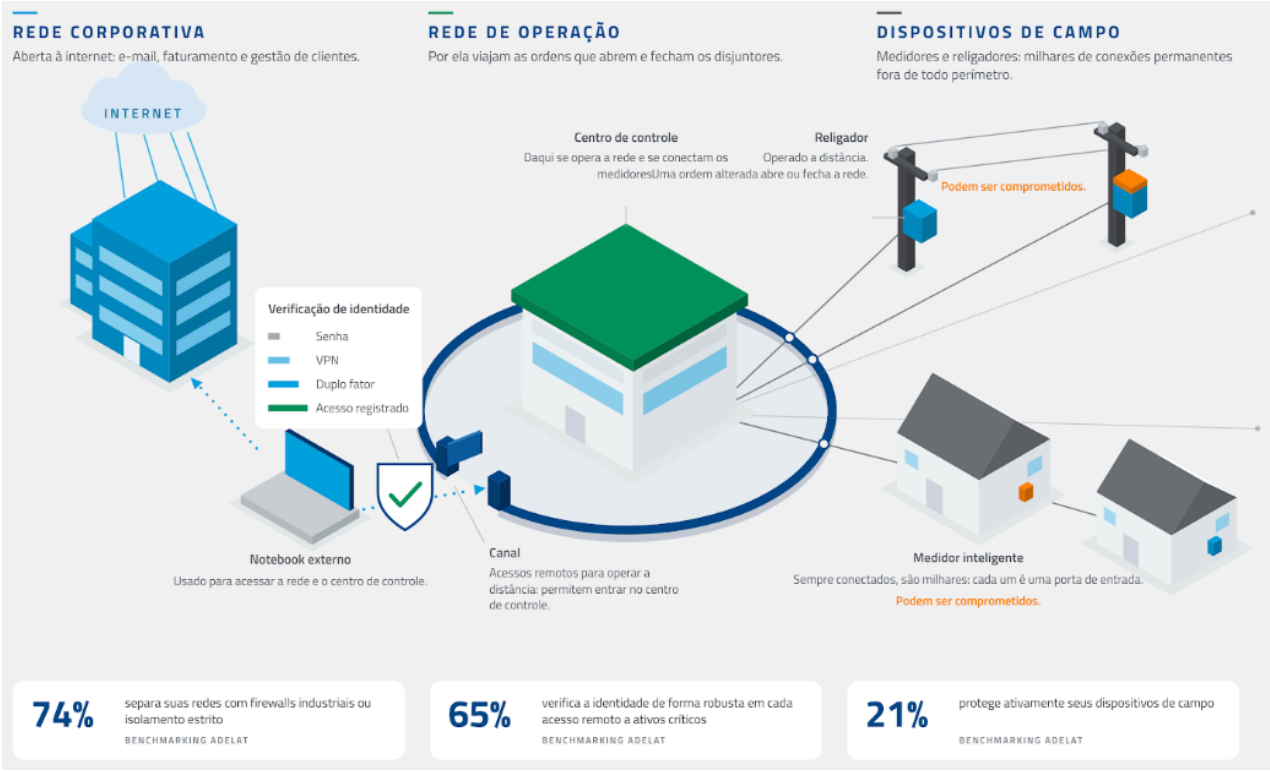


Fig. 2. As três frentes da infraestrutura de operação

3.2. CAPACIDADE DE DETECÇÃO E RESPOSTA

A vigilância consiste em examinar permanentemente os sinais que a infraestrutura gera. Os sistemas de uma distribuidora, os corporativos e os de operação, produzem alertas e registros a todo momento. Um centro de operações de segurança (SOC) é a unidade que os observa, os correlaciona e determina quais exigem resposta. As respostas das distribuidoras vão desde a ausência de qualquer monitoramento até um SOC especializado no setor elétrico, com analistas capazes de interpretar a operação da rede além dos sistemas corporativos, nível que alcançam 4 das 24 empresas que responderam. O dado que define a região está no outro extremo, porque os 17% que não contam com monitoramento ativo e os 29% que só vigiam a rede corporativa somam 46% do setor que não observa a rede de operação, de modo que uma intrusão nessa rede só é percebida quando já afeta o serviço. Quando isso ocorre, o que se mede deixa de ser a detecção e passa a ser a recuperação, quanto tempo a empresa leva para restabelecer o fornecimento e seus sistemas, essa duração se decide antes do incidente, com a existência de um plano de resposta que estabeleça quem decide, o que se desconecta e em que ordem o serviço é restabelecido. O espectro aqui separa duas coisas que costumam se confundir: ter o plano e tê-lo ensaiado, porque um plano jamais testado é apenas um documento e seu primeiro ensaio acaba sendo o incidente real. Um total de 43% das empresas valida o seu com simulações técnicas anuais, o dado mais alentador desta dimensão, apenas uma declara um plano coordenado com os organismos nacionais de cibersegurança ou defesa.

A análise avançada acrescenta à vigilância uma capacidade distinta: reconhecer comportamentos anômalos em vez de ameaças já conhecidas. A distinção importa porque os ataques mais graves contra redes elétricas não dependem de código estranho, mas de ordens legítimas emitidas por quem não deveria tê-las emitido. Diante de uma instrução válida em sua forma, a barreira não tem nada a objetar, o

que delata o intruso é o contexto, um disjuntor que se abre em um horário sem explicação ou uma sequência de manobras que nenhum operador executaria. Um sistema de detecção de anomalias aprende como é a operação normal da rede e alerta quando algo se afasta dela, a rede de operação é um terreno especialmente favorável para essa abordagem, porque seu tráfego é repetitivo e previsível, muito mais do que o corporativo, de modo que o incomum se destaca. O setor já está em movimento em direção a essa capacidade, pois das 22 empresas que responderam, 8 já a têm implementada, com sistemas em produção que monitoram o tráfego de rede e o correio eletrônico, outras 5 estão avaliando em pilotos ou provas de conceito, ensaios limitados que buscam comprovar seu desempenho no ambiente próprio antes de estendê-la à operação. No extremo superior, uma empresa declara modelos preditivos protegendo infraestrutura crítica.

O que unifica as três capacidades é que nenhuma pode ser tratada como uma obra concluída. Vigiar é um turno que não termina, um plano vale o que valeu seu último ensaio e os modelos de detecção são retreinados à medida que a rede muda. Não há aqui nada que possa ser construído uma vez, capitalizado e dado por encerrado, o próprio mercado confirma isso, porque das 13 empresas com monitoramento permanente de ambas as redes, 9 o contratam como serviço terceirizado, ou seja, uma fatura mensal e não um ativo. O desempenho reflete essa diferença, pois o monitoramento permanente de ambas as redes alcança 54% das empresas, o plano ensaiado 48% e a detecção de anomalias em operação 41%, enquanto a separação entre as redes corporativa e de operação, que se constrói uma vez e se financia como um investimento, chega a 74%. A terceirização já resolveu como prover essas capacidades mesmo para empresas de médio porte, de modo que a barreira não é tecnológica nem de oferta. O que ainda não foi resolvido é como pagá-las, porque uma assinatura de vigilância é exatamente o tipo de gasto recorrente que os marcos tarifários comprimem.



Fig. 3. As capacidades que administram o tempo do incidente

3.3. TERCEIROS, SERVIÇOS EM NUVEM E PROTEÇÃO DE DADOS

Uma parcela crescente da segurança e da operação de uma distribuidora é executada fora dela. O monitoramento é contratado como serviço, os sistemas são hospedados em nuvens de terceiros, os equipamentos chegam com o software de seu fabricante e os contratados acessam a rede para mantê-la, de modo que a exposição da empresa já não termina em sua própria infraestrutura. Essa extensão deixou de ser hipotética em 2023, quando vinte e duas empresas de energia dinamarquesas foram comprometidas simultaneamente por meio de uma vulnerabilidade nos equipamentos de um mesmo fornecedor. O ponto fraco não estava nas defesas de nenhuma delas, mas em um equipamento que todas haviam adquirido. O diagnóstico perguntou sobre as três faces desta frente: a segurança da cadeia de suprimentos, a proteção dos dados dos consumidores e a guarda das informações próprias.

A cadeia de suprimentos importa porque a empresa herda a segurança de tudo que compra. Cada sistema adquirido chega com o software de seu fabricante, cada contratado se conecta com suas próprias credenciais e cada serviço em nuvem repousa, por sua vez, em fornecedores que a distribuidora não escolheu nem conhece, uma opacidade que as próprias empresas descrevem entre suas maiores preocupações nas respostas abertas do diagnóstico. As práticas vão desde não avaliar o risco nas compras até submeter cada aquisição a testes técnicos de vulnerabilidade. Metade das empresas (12 de 24) situa-se no degrau contratual, com cláusulas de cibersegurança e direito de auditoria em seus contratos, apenas uma declara a validação técnica prévia. A diferença entre os dois degraus é a que separa o papel da verificação, porque a cláusula atribui responsabilidades e habilita a auditar, mas não examina o equipamento que está sendo comprado e o direito de auditar só protege se for exercido.

Os dados colocam o mesmo problema em duas direções. Para fora, a empresa custodia os registros de consumo de milhões de consumidores, que revelam rotinas e presença nos domicílios, um dano que, uma vez produzido, não pode ser desfeito. Para dentro, guarda informações valiosas para quem prepara uma intrusão: os projetos da rede, a localização de seus equipamentos e a configuração de seus sistemas, que em mãos erradas se convertem no mapa do ataque. Na primeira frente, 57% das empresas declaram alinhar-se à lei local de proteção de dados e apenas 26% acrescentam criptografia e controles de acesso rigorosos às suas bases comerciais. No segundo, metade se apoia no bloqueio de portas e periféricos, um controle físico para um problema que deixou de sê-lo, 6 de 21 mantêm vigilância ativa sobre a circulação de suas informações sensíveis. Em ambas as frentes, a maioria para onde termina a obrigação legal, as medidas que vão além desse mínimo, criptografar as bases e vigiar quais informações saem e por onde, continuam sendo a exceção.

As três faces desta frente repousam em instrumentos que se exercem uma vez: a cláusula é assinada, a declaração é solicitada, a lei é cumprida, uma vez exercidos podem ser dados por cumpridos. Verificar, por outro lado, é uma tarefa permanente, pois auditar o fornecedor, criptografar as bases e vigiar as informações que circulam é onde o setor para, porque metade das empresas assegura por contrato o que apenas uma comprova em campo, a maioria protege os dados de seus consumidores até onde a lei obriga, enquanto a criptografia continua sendo a exceção. A leitura regulatória tem duas faces. A primeira repete a do restante do capítulo: o esforço que se posterga é sempre o permanente. A segunda é nova, pois a proteção de dados pessoais é a frente onde a obrigação legal chegou primeiro e a mais países da região, é também a única onde a maioria das empresas converge para um padrão

comum. Onde houve norma, houve patamar mínimo; onde não há norma, a proteção fica a critério de cada empresa.

3.4. CULTURA ORGANIZACIONAL E TALENTOS ESPECIALIZADOS

As barreiras, os sistemas de vigilância e os contratos percorridos neste capítulo compartilham uma condição: todos são configurados e administrados por pessoas. Essa dependência tem duas frentes. A primeira abrange toda a organização, porque qualquer funcionário com um endereço de correio eletrônico é uma porta de entrada, a mensagem fraudulenta que consegue uma senha continua sendo um dos inícios mais frequentes de um ataque. A segunda é mais restrita e mais escassa: os sistemas de defesa exigem especialistas que compreendam ao mesmo tempo a segurança informática e a operação elétrica. O diagnóstico perguntou sobre ambas, a conscientização do pessoal em seu conjunto e a disponibilidade desse talento especializado.

A conscientização consiste em preparar todo o pessoal, não apenas o técnico, para reconhecer as tentativas de engano que chegam pelos canais cotidianos: o correio eletrônico, as mensagens, uma chamada telefônica. A formação vai desde sua completa ausência até uma cultura de segurança mensurada com indicadores por área e, no meio, está a distinção que importa: a diferença entre informar e treinar. As palestras ocasionais informam, mas o hábito de desconfiar se adquire praticando, por isso o padrão atual são as simulações de phishing[6], mensagens fraudulentas que a própria empresa envia a seu pessoal para medir quem as abre e reforçar quem cai. Um total de 44% das empresas já opera programas anuais com esse tipo de exercício e 12% adicional declara uma cultura contínua com indicadores de comportamento, enquanto os 44% restantes se dividem entre palestras ocasionais e a ausência de qualquer programa.

O talento especializado é o ponto onde o diagnóstico entrega seu resultado mais uniforme. A segurança de uma rede elétrica exige um perfil duplo: alguém que entenda os protocolos e os tempos da operação e, ao mesmo tempo, as técnicas de ataque e defesa informáticas, uma combinação escassa no mercado de trabalho em todo o mundo e que outras indústrias disputam com melhores salários. As respostas refletem isso sem nuances, pois 17 das 25 empresas, ou seja, 68%, declaram o mesmo estado: uma equipe estável, mas com lacunas de conhecimento em áreas específicas, com a tecnologia de operação entre as primeiras, nenhuma declara ter o perfil que precisa completamente coberto. As 8 restantes estão mais atrás: 5 sem pessoal especializado e 3 com dificuldades críticas para reter os que têm. É a resposta mais concentrada de todo o benchmarking.

As duas frentes compartilham a mesma economia. A formação só funciona quando repetida, porque o exercício deste ano não protege contra o engano do próximo, o especialista se paga todos os meses em um mercado que o disputa, de modo que ambas são gastos permanentes puros, sem nenhum ativo a mostrar em troca. A única diferença está no talento, cuja escassez não é de cada empresa, mas do mercado, razão pela qual é uma das poucas lacunas deste diagnóstico que o orçamento próprio não consegue fechar.

3.5. GOVERNANÇA, ORÇAMENTO E PAPEL DO CONSELHO

As quatro dimensões anteriores têm algo em comum: nenhuma se sustenta com uma decisão única. Renovar os controles, manter os turnos de vigilância, auditar os

[6] Phishing: Mensagem de correio eletrônico ou outro canal que se passa por um remetente legítimo para induzir o destinatário a entregar suas credenciais ou executar um arquivo malicioso.



Fig. 4. A dimensão humana, conscientização e talento

fornecedores e reter os especialistas exigem aprovações que se repetem a cada ano, essa continuidade só existe quando a segurança tem um lugar próprio no governo da empresa. O diagnóstico examinou esse lugar em três planos: quem responde pela segurança e perante quem, com quais recursos conta e com qual método é administrada.

O primeiro plano é o do responsável, as respostas se ordenam em quatro degraus conforme a autonomia da segurança e a quem ela reporta. No mais baixo, não existe atribuição formal, situação em que se encontra apenas uma empresa. No segundo, a responsabilidade é delegada à chefia de tecnologia da informação, aí permanece quase metade do setor: 12 das 25 empresas. No terceiro, existe um cargo dedicado, um chefe ou gerente de segurança que ainda reporta dentro da área de tecnologia, com 6 empresas. No mais alto, que outras 6 alcançam, há um CISO, a figura executiva que reporta diretamente à diretoria geral ou ao conselho. A ascensão importa porque cada degrau aproxima a segurança de quem decide, pois quem reporta dentro de tecnologia compete pelo orçamento de tecnologia e chega ao conselho com sua mensagem filtrada, enquanto o CISO defende seu gasto sem intermediários. A perspectiva se completa com a frequência com que o conselho recebe o tema, onde 8 das 22 empresas que responderam só recebem informes após um incidente grave, quando já não há nada a decidir, mas apenas quanto custou; 10 o integram semestralmente à sua matriz de riscos corporativos e apenas uma mantém reporte trimestral com indicadores. Em suma, a região já instalou o cargo, mas ainda não lhe dá o nível hierárquico, pois metade das empresas trata a cibersegurança como mais uma função informática e apenas uma em cada quatro a posiciona onde as decisões são tomadas.

O segundo plano é o do orçamento, o que

o diagnóstico revela não é um problema de magnitude, mas de visibilidade. Em 6 das 20 empresas que responderam, o gasto em cibersegurança não existe como rubrica própria, distribui-se entre outras contas, um gasto sem linha não se planeja nem se defende, negocia-se a cada ano contra tudo o mais e é o primeiro a ceder quando o orçamento é ajustado. A evidência de que a condição é a rubrica e não o valor está nas demais, pois das 14 que individualizaram o gasto, 12 já destinam ao menos 3% de seu orçamento de tecnologia a ele. Quando a segurança consegue existir como rubrica, o financiamento a acompanha. Fora da empresa o problema se repete: a tarifa também não individualiza esse gasto. O que não se individualiza não se financia.

O terceiro plano é o do método, aí o setor mostra mais avanço do que costuma ser reconhecido. Sete empresas operam com certificação vigente ou auditoria externa sob normas internacionais, metade já mede seu desempenho com indicadores operacionais, quanto tempo leva para detectar uma intrusão e quanto para responder. O que falta está no final da cadeia, na quantificação do risco, porque traduzir a probabilidade e o impacto de um ataque em termos econômicos é uma prática que declara apenas uma das 23 empresas que responderam. As demais avaliam seu risco com matrizes e escalas qualitativas, úteis para ordenar prioridades internas, mas silenciosas perante quem decide com números. Essa tradução pendente explica boa parte desta dimensão, porque um conselho compara investimentos em dinheiro, um risco que não se expressa em dinheiro compete por orçamento como um ato de fé. O que vale para o conselho vale para o regulador, que tampouco pode reconhecer na tarifa um custo que a própria indústria ainda não quantifica.

Os três planos contam a mesma história em níveis distintos. A segurança já tem cargo, mas raramente tem nível hierárquico; já tem gasto, mas muitas vezes sem rubrica; e já tem método, mas ainda não fala o idioma em que se decidem os investimentos. Nada disso é casual, porque as quatro dimensões anteriores mostraram que as lacunas do setor se concentram onde a proteção exige gasto permanente e, um gasto permanente só sobrevive se alguém com poder o aprova a cada ano, com uma rubrica a partir da qual defendê-lo e um valor de risco que o justifique. Por isso a maturidade técnica de uma distribuidora nunca supera por muito tempo a governança que a financia. Mas a governança interna tem um limite que este capítulo deixa estabelecido: pode decidir gastar, mas não pode decidir que esse gasto seja reconhecido na tarifa. Essa decisão pertence ao regulador e a ela se dedicam os capítulos seguintes.

> “Quando a segurança consegue existir como rubrica, o financiamento a acompanha.

04

A RESPOSTA REGULATÓRIA NA AMÉRICA LATINA

Diante de um panorama de maturidade desigual, no qual os avanços técnicos das empresas ainda não contam com a governança nem o financiamento que os sustentem ao longo do tempo, os marcos regulatórios da região começaram a se mover, embora em ritmos e com abordagens distintas entre países. Este capítulo examina como o ambiente normativo latino-americano está respondendo aos riscos de cibersegurança no setor elétrico.

O Capítulo 3 documentou uma maturidade desigual e, sobretudo, incompleta: as empresas avançam em controles técnicos, mas essa capacidade não está sustentada por governança formal, orçamento diferenciado nem reconhecimento econômico. Cabe agora perguntar o que a regulação está fazendo diante dessa lacuna. Este capítulo deixa de lado o diagnóstico das empresas, já coberto, e examina o diagnóstico das normas: quais instrumentos regulatórios existem hoje na região, a quem obrigam, o que exigem e, sobretudo, se reconhecem o custo de cumpri-los. A primeira seção mapeia o panorama regulatório regional em seu conjunto e expõe as tensões que surgem quando a norma avança em ritmo diferente da capacidade operacional das empresas que deve regular. A segunda seção desagrega esse panorama país a país, destacando como casos como os do Brasil e do Chile, pioneiros em estabelecer obrigações setoriais vinculantes, convivem com realidades operacionais muito distintas e, como outros países da amostra, avançam ainda sobre a base de marcos gerais que nem sempre alcançam a distribuição elétrica privada ou cooperativa.

4.1. O CONTEXTO

Dos países analisados, três contam hoje com uma obrigação setorial elétrica de cibersegurança vinculante e exigível para a distribuição: Brasil e Chile por meio de lei e regulação estatal e Colômbia por meio de um acordo obrigatório do operador do sistema, sem necessidade de uma lei geral de cibersegurança. O restante da amostra se apoia em marcos gerais de cibersegurança, em esquemas exclusivos para o setor público ou carece completamente de norma dedicada. Essa assimetria, dois países com obrigação setorial firme e nove sem ela, é o primeiro dado que qualquer proposta regulatória deve tomar como ponto de partida e é detalhada país a país na seção seguinte.

A região compartilha, sem exceção, um mesmo vazio: nenhum dos marcos regulatórios reconhece a cibersegurança como uma rubrica tarifária explícita e autônoma. Onde a obrigação existe, o custo de cumpri-la se dilui em rubricas genéricas de operação, manutenção ou investimento. Essa é a tensão regulatória mais relevante para uma associação de distribuidoras, porque significa que a norma pode exigir um controle sem abrir, ainda, a via para financiá-lo.

Uma segunda tensão aparece entre a exigência técnica e seu reconhecimento regulatório. O Chile é o país que mais avançou na construção do aparato normativo, com lei marco, agência fiscalizadora, CSIRT[7] nacional e uma norma técnica elétrica própria, tudo em menos de dois anos (2024-2026), mas esse mesmo marco ainda não contempla o reconhecimento tarifário dos

[7] CSIRT: Computer Security Incident Response Team – equipe especializada que recebe as notificações de incidentes, coordena a resposta e difunde alertas entre as organizações de seu âmbito.

investimentos que exige. O cumprimento técnico, em outras palavras, pode tornar-se obrigatório antes que exista a regulação econômica que o sustente.

Uma terceira tensão é de sequência: a norma setorial pode chegar antes da capacidade operacional de quem ela obriga. O Brasil foi o primeiro país da região a editar uma norma setorial elétrica vinculante (ANEEL 964/2021, vigente desde 2022), mas a aplica de forma uniforme a distribuidoras de porte e capacidade muito distintos, sem diferenciar o ritmo de exigência conforme o tamanho da empresa obrigada. É o risco regulatório inverso ao do Chile: enquanto lá a arquitetura institucional corre à frente do financiamento, no Brasil a obrigação corre à frente da capacidade das empresas menores para cumpri-la.

Essas três tensões, o vazio tarifário universal, a exigência técnica sem financiamento e a norma sem diferenciação por capacidade, não se distribuem de igual maneira entre os onze países. A América Latina não avança no mesmo ritmo em matéria de cibersegurança elétrica, mas tampouco avança em direções desconectadas entre si. Um panorama dos onze países analisados revela três grupos com perfil próprio: um núcleo maduro formado por Brasil, Chile e Colômbia, onde a norma setorial já alcança as distribuidoras de forma vinculante; um grupo intermediário, Peru, Argentina e Equador, que em apenas dois anos construiu uma institucionalidade nacional ainda não totalmente aplicada ao setor elétrico; e um grupo inicial, Costa Rica, El Salvador, Guatemala, Bolívia e Paraguai, que está apenas começando a discutir quem deve governar o tema.

O mais revelador, contudo, não é a distância entre esses grupos, mas o que todos compartilham. Nenhum país da região, nem mesmo os mais avançados, reconhece a cibersegurança como uma rubrica tarifária explícita e autônoma. Os custos, quando existem, se diluem em rubricas genéricas de operação, manutenção ou planos de investimento. Esse é o achado mais relevante, ou seja, o marco legal avança, mas o marco econômico que deveria sustentá-lo ainda não existe em nenhum lugar.

O quadro comparativo deixa cinco constatações que convém fixar antes do percurso país a país:

- Ausência total de uma rubrica tarifária de cibersegurança. Em nenhum dos onze países a cibersegurança aparece como componente tarifário reconhecido de forma explícita e autônoma.
- A obrigatoriedade setorial elétrica só é clara e madura no Brasil, no Chile e na Colômbia, onde a norma menciona expressamente as distribuidoras e fixa prazos ou um regime sancionatório.
- Um regime sancionatório realmente ativo só existe no Chile, com multas para operadores de importância vital de até 40.000 UTM (Unidades Tributárias Mensais) desde março de 2025.
- A obrigação de notificar incidentes já alcança também Peru e Equador, embora em ambos os casos sem regime sancionatório plenamente exigível ainda.
- Existe CSIRT (Computer Security Incident Response Team; equipe de resposta a incidentes de segurança informática) nacional em quase todos os países, mas um CSIRT setorial elétrico formal apenas na Colômbia; no Chile, a função é cumprida de facto pela unidade especializada do CEN (Coordinador Eléctrico Nacional).

4.2. EVOLUÇÃO POR PAÍS

País	Norma setorial de cibersegurança elétrica?	Alcança a distribuição?	Obrigação de notificação de incidentes?	CSIRT nacional ou setorial?	Investimentos reconhecidos na tarifa?
Brasil	Sim – REN ANEEL 964/2021, com fiscalização ativa desde fev/2025 (Despacho 427: envio periódico de dados de monitoramento)	Sim – concessionárias, permissionárias, autorizadas e demais agentes (G, T, D, operação do sistema e comercialização)	Sim – notificação ao CTIR Gov assim que o incidente é identificado, com análise de causa, impacto e mitigação	CSIRT nacional (CTIR Gov); sem CSIRT setorial elétrico dedicado formal	Não identificado – sem rubrica tarifária explícita e autônoma
Chile	Sim – Lei 21.663/2024 + Padrão de Cibersegurança do CEN (base NERC-CIP – 2022); NTSyCS da CNE	Sim – G, T e D qualificadas como serviços essenciais; abrange toda a cadeia, inclusive o próprio CEN	Sim – art. 9° Lei 21.663: alerta precoce 3h, relatório inicial 72h, relatório final 15 dias (Decreto 295)	Sim – CSIRT Nacional + CSIRT de Defesa; no setor elétrico, a Unidade de Cibersegurança do CEN funciona de facto como equipe setorial	Não – sem reconhecimento tarifário explícito e autônomo; custos absorvidos na regulação geral de operação e investimento
Colômbia	Sim – Guia de Cibersegurança do CNO, Acordo 1960/2025, com abordagem de risco e prazos escalonados até 2028	Sim – obrigatório para G, T, D e o operador do SIN (Sistema Interconectado Nacional)	Sim – Acordo CNO 2088 (nov/2025)	Sim – colCERT (CSIRT nacional; Decreto 338/2022) + CSIRT setorial elétrico	Não – a Res. CREG 101-001/2022 trata a Cibersegurança da medição avançada como obrigação técnica
Argentina	Não – sem norma do ENRE; Decisão Administrativa 641/2021 e a Disposição 1/2026 do novo Centro Nacional de Cibersegurança aplicam-se apenas ao Setor Público Nacional	Não se aplica diretamente (distribuidoras privadas não vinculadas)	Não – sem prazo legal fixo nem regime sancionatório para distribuidoras privadas	Parcial – CERT.ar (CSIRT nacional)	Não – sem reconhecimento tarifário na metodologia do ENRE
Peru	Não – sem norma dedicada, apenas normas técnicas conexas que referenciam NERC-CIP (SCADA e disponibilidade)	Parcial – as normas conexas cobrem SCADA e disponibilidade, sem constituir regulação de cibersegurança propriamente dita	Sim – Decreto Supremo 126-2025-PCM (regulamento do DU 007-2020, vigente desde fev/2026), fixa 48h para notificar ao CNSD; regime sancionatório ainda pendente	Sim – PECERT (CSIRT nacional, operado pelo Centro Nacional de Segurança Digital); sem CSIRT setorial elétrico formal	Parcial e casuístico – sem reconhecimento tarifário estruturado
Equador	Sim, desde 2026 – Lei Orgânica para o Fortalecimento da Cibersegurança	Parcial – energia reconhecida como setor essencial; classificação efetiva prevista entre nov/2026 e mai/2027	Sim – obrigação de notificar em 72h já vigente, sem órgão de controle setorial designado; regime sancionador pleno exigível em 24 meses	Sim – CSIRT Nacional com autonomia operativa, ainda sem articulação formal com o setor elétrico	Não – metodologia estruturada em ativos físicos, sem categoria equivalente para proteção digital
Costa Rica	Não – sem norma setorial elétrica	Não se aplica	Não – a Diretriz 133-MP-MICITT exige notificação ao CSIRT-CR apenas na Administração Pública Central	Sim – CSIRT-CR (nacional, operativo)	Não identificado

País	Norma setorial de cibersegurança elétrica?	Alcança a distribuição?	Obrigação de notificação de incidentes?	CSIRT nacional ou setorial?	Investimentos reconhecidos na tarifa?
El Salvador	Parcial – Decreto 143/2024 alcança infraestruturas críticas (incl. energia), sem norma própria	Sim, em princípio (pendente de diretrizes técnicas)	Depende de regulamentação futura da ACE	Sim – Agência de Cibersegurança do Estado, nacional; sem CSIRT setorial elétrico identificado	Não identificado
Guatemala	Não – sem lei geral vigente; Iniciativa 6347 em tramitação, objeto de debate público e ainda não aprovada	Não se aplica	Não – sem obrigação legal vigente de notificação	Não – sem CSIRT nacional consolidado; sem CSIRT setorial elétrico	Não existe mecanismo explícito de reconhecimento tarifário para investimentos e gastos recorrentes de cibersegurança
Bolívia	Não – sem lei geral nem estratégia nacional aprovada	Não se aplica	Não – sem prazo definido nem regime sancionatório	Parcial – CSIRT-BO (CSIRT nacional); sem CSIRT setorial elétrico	Não identificado
Paraguai	Não – sem norma setorial elétrica dedicada	Não se aplica	Não identificado	Sim – CERT-PY (nacional); sem CSIRT setorial elétrico	Não identificado

Tabela 4.1. Marco regulatório de cibersegurança elétrica por país.

O núcleo maduro: Brasil, Chile e Colômbia. Esses três países chegaram à maturidade regulatória por caminhos distintos, aí reside parte de seu interesse. O Brasil o fez da forma mais direta: o regulador elétrico, a ANEEL (Agência Nacional de Energia Elétrica), emitiu sua própria resolução normativa (964/2021) e hoje fiscaliza ativamente seu cumprimento, exigindo desde 2025 o envio periódico de dados sobre maturidade e riscos. O Chile combinou uma lei marco nacional, a Lei 21.663, vigente desde março de 2025, com um regime sancionatório real e multas de até 40.000 UTM, com um padrão técnico próprio que o Coordenador Elétrico Nacional (CEN) vem aplicando desde 2020, inspirado no NERC-CIP (North American Electric Reliability Corporation – Critical Infrastructure Protection) norte-americano. A Colômbia, por sua vez, chegou a um desenvolvimento setorial comparável sem ter lei geral de cibersegurança: o Conselho Nacional de Operação (CNO) construiu, a partir de sua própria competência regulamentar, um guia obrigatório para toda a cadeia elétrica e, em novembro de 2025, um CSIRT setorial próprio.

Essa última observação, um país sem marco nacional que ainda assim lidera em maturidade setorial, é talvez a sincronia mais interessante do grupo: demonstra que a autorregulação de um operador do sistema com competência normativa pode avançar mais rapidamente do que uma lei geral e que ambos os caminhos convergem, cedo ou tarde, para resultados semelhantes: cobertura de toda a cadeia, prazos de notificação definidos e um CSIRT dedicado ao setor.

Ainda assim, nenhum dos três resolveu o nó tarifário. O Brasil deixa aberta a possibilidade de que a ANEEL avalie no futuro um reconhecimento de custos; o Chile e a Colômbia, por ora, não o contemplam.

O grupo intermediário e a janela 2025-2026. Peru, Argentina e Equador reorganizaram sua institucionalidade de cibersegurança quase ao mesmo tempo, no período final de 2025 e início de 2026. A Argentina

criou seu Centro Nacional de Cibersegurança por decreto de necessidade e urgência em 31 de dezembro de 2025, vigente desde janeiro de 2026. O Peru finalmente regulamentou, após cinco anos de vigência parcial, seu Decreto de Urgência 007-2020, com um regulamento publicado em novembro de 2025 e vigente desde fevereiro de 2026, que fixa um prazo de 48 horas para notificar incidentes. O Equador aprovou no mesmo período sua primeira lei orgânica integral de cibersegurança. Até a Bolívia, que se encontra em uma etapa mais inicial de desenvolvimento institucional, moveu sua institucionalidade nesse mesmo período: o Decreto Supremo 5519, de janeiro de 2026, transferiu as competências de certificação digital da ADSIB para a AGETIC.

Essa coincidência temporal, quatro países reformando sua arquitetura institucional em uma janela de apenas três meses, sugere algo mais do que casualidade: provavelmente responde a uma pressão regional comum, seja normativa, geopolítica ou derivada de incidentes recentes, que empurrou vários governos a agir quase simultaneamente.

O que ainda não ocorreu, em nenhum dos três países intermediários, é que essa institucionalidade nacional chegue ao setor elétrico. No Peru, o regulador Osinergmin e o operador COES seguem sem uma norma de cibersegurança propriamente dita, apoiando-se apenas em referências técnicas ao NERC-CIP. Na Argentina, a normativa vigente rege apenas o Setor Público Nacional e não vincula as distribuidoras privadas, salvo adesão voluntária. No Equador, a lei já reconhece a energia elétrica como serviço essencial, mas a classificação efetiva dos ativos e empresas sujeitos ao regime só ocorrerá entre novembro de 2026 e maio de 2027.

O grupo inicial: entre a estratégia e a regulação a construir. Costa Rica, El Salvador, Guatemala, Bolívia e Paraguai compartilham uma característica comum: nenhum conta ainda com uma norma setorial elétrica dedicada. Mas mesmo aqui aparecem paralelismos que valem ser destacados. Costa Rica e El Salvador avançam pela mesma via: um projeto de lei que criaria uma agência nacional de cibersegurança. Na Costa Rica, o Expediente 23.292 está em tramitação desde agosto de 2022 e prevê explicitamente a articulação da futura agência com reguladores setoriais como a ARESEP. El Salvador já cruzou essa meta: seu Decreto 143/2024 criou a Agência de Cibersegurança do Estado, mas a aplicação ao setor elétrico continua pendente de diretrizes técnicas que a própria agência ainda não emitiu. É, de certa forma, a mesma história contada em dois momentos distintos.

Outra sincronia une Chile, El Salvador e Equador, países muito distantes em maturidade: os três aprovaram sua lei de cibersegurança quase simultaneamente com uma lei de proteção de dados pessoais. Essa duplicidade não é casual: ambas as matérias compartilham fatos geradores (uma violação de dados costuma ser também um incidente cibernético) e, em vários países, já gera um risco concreto de notificação duplicada perante autoridades distintas, algo que o próprio texto do Equador aponta expressamente.

O Paraguai merece menção separada por sua singularidade estrutural: ao não ter um regulador elétrico independente, pois o sistema é operado pela estatal ANDE, verticalmente integrada, nem faz sentido perguntar sobre reconhecimento tarifário, porque não existe um processo de revisão tarifária regulada ao qual esse reconhecimento pudesse se aplicar. É o único país dos onze onde o vazio tarifário não é uma omissão regulatória, mas uma consequência direta do design institucional do setor.

Guatemala e Bolívia encontram-se, dentro deste grupo, em uma etapa mais inicial de desenvolvimento institucional: nenhum conta com lei geral aprovada, CSIRT nacional plenamente consolidado nem classificação de infraestrutura crítica. A Guatemala apresenta ainda uma particularidade

própria: seu projeto de lei (Iniciativa 6347) é objeto de debate público, sem que exista ainda consenso sobre qual órgão deveria exercer a governança do tema.

Além dos grupos de maturidade, o corpus regulatório da região deixa ver alguns padrões que se repetem de um país a outro:

1. **A janela 2025–2026.** Colômbia (Acordo CNO 2088, nov/2025), Peru (regulamento do DU 007-2020, nov/2025, vigente em fev/2026), Argentina (criação do Centro Nacional de Cibersegurança, dez/2025, vigente em jan/2026) e Bolívia (transferência de funções para a AGETIC, jan/2026) reformaram sua institucionalidade em um intervalo de apenas três meses. É o sinal mais claro de que o tema ganhou urgência política de forma simultânea em governos que, em quase tudo o mais, avançam em ritmos distintos.

2. **Um padrão emprestado como âncora técnica.** O NERCCIP norteamericano aparece como referência técnica tanto no padrão chileno do CEN (2020) quanto nas normas técnicas conexas do setor elétrico peruano. Nenhum outro padrão internacional se repete com essa frequência nos textos analisados, o que sugere uma via de convergência técnica de fato, mesmo onde não há convergência legal.

3. **Leis gêmeas: cibersegurança e dados pessoais.** Chile, El Salvador e Equador aprovaram sua lei de cibersegurança junto com uma lei de proteção de dados pessoais, quase como um pacote único. Essa proximidade normativa multiplica as obrigações de notificação para um mesmo incidente e antecipa um problema de coordenação institucional que nenhum país, por ora, resolveu completamente.

4. **CSIRT nacional quase universal, CSIRT elétrico quase inexistente.** Dez dos onze países contam com um CSIRT nacional operacional (CTIR Gov, CSIRT Nacional/Chile, colCERT, CERT.ar, PECERT, CSIRT Equador, CSIRTCR, CSIRTBO, CERTPY; El Salvador é a exceção visível, com seu registro de incidentes sob a ACE). Mas um CSIRT dedicado ao setor elétrico só existe, de forma plenamente formal, na Colômbia; o Chile o possui de fato por meio do CEN. O restante da região continua dependendo de equipes genéricas para incidentes que, por sua natureza, exigem conhecimento operacional específico de subestações, SCADA[8] e telecontrole.

5. **O vazio tarifário, sem exceções.** É o único ponto em que os onze países coincidem sem nuances: em nenhum deles a cibersegurança é uma rubrica tarifária explícita e autônoma de custo ou investimento remunerado. Mesmo onde o marco legal é mais exigente — Chile e Colômbia, o financiamento dessas obrigações segue sem uma via formal de reconhecimento.

O panorama regional deixa uma leitura dupla. Por um lado, há um movimento regulatório real e, em vários casos, coordenado no tempo: a janela 2025-2026 mostra que vários governos estão levando o tema a sério de forma quase simultânea e os três países mais maduros já cobrem as distribuidoras com obrigações concretas de notificação e, ao menos no Chile, sanções efetivas. Por outro lado, a região inteira compartilha um mesmo ponto cego: o design tarifário não evoluiu no mesmo ritmo que o design normativo. Enquanto isso não mudar, as distribuidoras continuarão investindo em cibersegurança sem uma via formal para recuperar esse custo, uma lacuna que cedo ou tarde terá de ser fechada em todos os países.

[8] SCADA: Supervisory Control and Data Acquisition – sistema que supervisiona e comanda remotamente os equipamentos da rede elétrica a partir de um centro de controle.

05

ABORDAGENS REGULATÓRIAS INTERNACIONAIS E MELHORES PRÁTICAS

O capítulo anterior constata que a regulação de cibersegurança elétrica está se movendo na América Latina, mas de forma desigual, com instrumentos dispersos e sem resolver quem paga a proteção de uma rede que a própria regulação obriga a digitalizar.

Este capítulo revisa seis jurisdições que levam entre seis e dezoito anos regulando a cibersegurança de seus sistemas elétricos: Estados Unidos, União Europeia, Reino Unido, Austrália, a província canadense de Ontário e Índia. É importante advertir que os referenciais examinados operam sobre premissas institucionais que na região nem sempre se cumprem: reguladores com capacidade técnica própria para auditar cibersegurança industrial, agências nacionais de cibersegurança consolidadas e marcos tarifários com revisões periódicas onde uma rubrica nova pode efetivamente entrar.



Para que a comparação seja útil e não se converta em um catálogo, cada jurisdição é examinada com as mesmas quatro perguntas: (i) O que exige? Se a obrigação é um controle técnico verificável, um sistema de gestão ou um nível de maturidade avaliado; se é voluntária ou obrigatória e com que consequência por descumprimento; (ii) A quem alcança? Se cobre apenas o sistema de transmissão ou também a distribuição e com que critério se define o universo obrigado: porte, criticidade, impacto ou número de consumidores; (iii) Como se financia? Qual instrumento reconhece o custo do cumprimento: rubrica tarifária, incentivo, ativo regulatório, caso de negócio ou nenhum; (iv) Como se gradua? O mecanismo de proporcionalidade que permite que uma cooperativa rural e um grande grupo convivam sob a mesma norma sem que a primeira fique excluída nem a segunda seja sub-exigida.

A regulação de cibersegurança elétrica do mundo desenvolvido nasceu observando o sistema de transmissão. Estados Unidos, União Europeia e Austrália construíram seus marcos em torno do risco sistêmico do sistema atacadista, a distribuição entrou depois, de forma parcial, tardia ou indireta. Apenas três dos sete casos revisados foram escritos pensando explicitamente em distribuidoras, dois deles são dos últimos três anos. Para a América Latina, isso tem uma leitura animadora: a região não chega tarde a um modelo consolidado, porque o modelo regulatório para a distribuição ainda está sendo escrito em todo o mundo.

5.1. ESTADOS UNIDOS: OBRIGATORIEDADE FEDERAL PARA O SISTEMA ATACADISTA, VOLUNTARIEDADE ESTADUAL PARA A DISTRIBUIÇÃO

A regulação elétrica norte-americana distribui competências por segmento e não por território. A Comissão Federal Reguladora de Energia tem jurisdição sobre a transmissão interestadual e a venda atacadista de eletricidade, enquanto a distribuição e o fornecimento no varejo ficam sob as comissões reguladoras de cada estado. Essa divisão, anterior a qualquer discussão sobre cibersegurança, determina o alcance do regime federal e explica por que o país com as exigências mais rígidas do mundo para o sistema atacadista carece de um marco obrigatório único para a distribuição.

A segunda particularidade é institucional. Após o apagão no nordeste de 2003, a legislação federal criou a figura da organização de confiabilidade elétrica: uma entidade privada certificada pelo regulador federal, com competência para propor padrões que, uma vez aprovados, adquirem força obrigatória para todos os usuários, proprietários e operadores do sistema atacadista. A organização designada, a NERC, edita os padrões e verifica seu cumprimento por meio de entidades regionais que auditam mais de mil entidades cadastradas. É um modelo de corregulação: a indústria redige a norma técnica, o regulador a aprova e lhe confere força vinculante e a sanção é pública.

NERC CIP: padrões obrigatórios, auditáveis e sancionáveis

Em 2008, a Comissão aprovou a primeira família de padrões de proteção de infraestrutura crítica, conhecidos como NERC CIP. O conjunto está organizado por matérias e cresceu de forma contínua durante quase duas décadas. Parte da identificação e classificação dos sistemas cibernéticos do sistema atacadista e, a partir daí, desdobra requisitos sobre controles de gestão de segurança, pessoal e capacitação, perímetros eletrônicos de segurança, segurança física dos ativos cibernéticos, gestão de sistemas e de correções de software, notificação de incidentes e planos de resposta, planos de recuperação, gestão de mudanças e avaliações de vulnerabilidade, proteção da informação e, desde 2020, gestão do risco da cadeia de suprimentos.

Não são guias de boas práticas, mas normas exigíveis. O cumprimento é verificado mediante auditorias periódicas conduzidas pelas entidades regionais, complementado pela obrigação de autorreportar os próprios descumprimentos e de apresentar planos de mitigação, respaldado por sanções civis que podem alcançar a ordem de USD 1,5 milhão por dia e por infração. A sanção é ainda pública: os expedientes e os valores são publicados, de modo que ao custo econômico se soma um custo reputacional.

A proporcionalidade está incorporada no próprio design. Cada sistema cibernético é classificado em três níveis de impacto, alto, médio e baixo, conforme as consequências que seu comprometimento teria sobre o sistema, o conjunto de requisitos aplicáveis depende dessa classificação e não do porte da empresa que o opera. Um centro de controle de grande capacidade e uma instalação menor ficam sujeitos a exigências distintas, ainda que pertençam à mesma companhia.

A evolução mais recente confirma o deslocamento da defesa para o interior da rede. Em junho de 2025, a Comissão aprovou o padrão CIP-015, que obriga a monitorar o tráfego dentro dos perímetros eletrônicos de segurança e não apenas em suas bordas, com prazos escalonados de trinta e seis meses para os centros de controle e sessenta para o restante dos ativos aplicáveis. O fundamento declarado é que as defesas perimetrais não detectam o atacante que já obteve acesso legítimo e que

reconhecer o movimento lateral[9] a tempo é a única forma de limitar o dano.

A Ordem 893 e a calibração dos incentivos

O precedente norte-americano mais relevante em matéria de financiamento nasceu por mandato legislativo. A lei de infraestrutura de 2021 incorporou à lei federal de energia um artigo que ordenou à Comissão estabelecer, por regulamento, um tratamento tarifário incentivado para os investimentos em cibersegurança avançada. O resultado foi a Ordem 893, de abril de 2023.

O design reconhece duas coisas. A primeira é que a cibersegurança tem um componente substancial de gasto recorrente e não apenas de investimento: entre os conceitos elegíveis figuram gastos de operação e manutenção, custos de pessoal, implementação, monitoramento de rede, capacitação e determinados serviços contratados na modalidade de assinatura. A segunda é que o esforço que excede o cumprimento obrigatório merece um reconhecimento diferenciado, de modo que o incentivo se reserva para investimentos voluntários que melhorem de forma material a posição de segurança e que não estejam já exigidos pelos padrões CIP.

O instrumento finalmente aprovado foi um ativo regulatório de cibersegurança que permite diferir esses custos, incorporá-los à base tarifária e obter retorno sobre a parcela não amortizada, com um prazo de amortização de até cinco anos. A proposta original contemplava também um adicional sobre a rentabilidade reconhecida, que a Comissão descartou na resolução final. O acesso foi estruturado sobre uma lista de conceitos pré-aprovados que ficou reduzida a dois: a participação no programa federal de intercâmbio de informações sobre ameaças e o desdobramento de monitoramento interno da rede.

Mais de um ano após sua entrada em vigor, nenhuma solicitação havia sido apresentada. O diagnóstico dos analistas do setor aponta para a combinação de uma lista pré-aprovada demasiadamente estreita, um procedimento que exige uma apresentação tarifária específica passível de impugnação por terceiros e um benefício que para a maioria das empresas não compensava esse custo administrativo. O caso é útil precisamente por isso: mostra que o reconhecimento tarifário da cibersegurança não se resolve com a existência do instrumento, mas com sua calibração.

O vazio da distribuição e a resposta NARUC-DOE

O alcance do NERC CIP é o sistema elétrico atacadista. A distribuição permanece sob competência dos reguladores estaduais, com resultados marcadamente heterogêneos: alguns estados desenvolveram exigências próprias ou figuras de supervisão especializada, outros incorporam a cibersegurança como critério dentro dos processos tarifários ordinários e outros não legislaram sobre o tema.

Diante dessa dispersão, a resposta não foi uma norma federal, mas um produto de referência construído em um processo público-privado. Em fevereiro de 2024, a associação nacional de reguladores estaduais e o Departamento de Energia publicaram um conjunto de linhas de base de cibersegurança para sistemas de distribuição e para os recursos energéticos distribuídos que se conectam a eles, elaborado por um grupo diretivo integrado por reguladores estaduais, distribuidoras, operadores e agregadores de recursos distribuídos e especialistas em segurança.

O produto não tem natureza de padrão. É uma linha de base dirigida a três públicos distintos, as comissões estaduais, as distribuidoras e os operadores de recursos distribuídos, seu objetivo declarado é o alinhamento entre os estados que decidam

[9] Movimento lateral: deslocamento de um atacante do sistema pelo qual obteve acesso para outros sistemas da mesma organização, aproveitando acessos e credenciais legítimos.

adotá-la, qualquer que seja a via pela qual o façam. Uma segunda fase, desenvolvida durante 2025, produziu guias de implementação centradas nos dois problemas que a experiência mostrou como críticos: a delimitação do universo de ativos a considerar e a priorização entre as medidas da linha de base, com percursos diferenciados conforme a adoção seja voluntária ou obrigatória e conforme o porte, a titularidade e a maturidade de cada empresa.

5.2. UNIÃO EUROPEIA: DA NORMA HORIZONTAL AO CÓDIGO DE REDE SETORIAL

A regulação europeia de cibersegurança elétrica se constrói sobre dois instrumentos jurídicos de natureza distinta. As diretivas fixam objetivos e devem ser transpostas para a legislação de cada Estado-Membro, o que introduz variabilidade e tempo, enquanto os regulamentos são de aplicação direta e uniforme. A cibersegurança do setor elétrico europeu ficou regulada por ambos, uma diretiva transversal que cobre todos os setores críticos e um regulamento setorial que se aplica diretamente à eletricidade.

A segunda particularidade é o instrumento escolhido para o nível setorial. Os códigos de rede são o mecanismo com que a União harmoniza as regras técnicas do mercado interno de eletricidade, conexão, operação, equilíbrio e gestão de capacidade, são elaborados mediante um procedimento em que participam a Comissão, a agência de cooperação dos reguladores de energia, a rede europeia de operadores de transmissão e a entidade europeia de operadores de distribuição. Que a cibersegurança tenha sido incorporada por essa via significa que ela é tratada como uma condição de operação do sistema, no mesmo plano que as regras de frequência ou de equilíbrio, e que seu desenvolvimento técnico corre por conta dos mesmos atores que operam a rede.

NIS2 e o Código de Rede: duas camadas normativas

A diretiva de segurança das redes e sistemas de informação de 2022, conhecida como NIS2, fixa o patamar comum. Alcança as entidades consideradas essenciais, entre elas as do setor energético, lhes impõe gestão de riscos, notificação de incidentes em prazos curtos, segurança da cadeia de suprimentos e responsabilidade dos órgãos de direção pela supervisão dessas medidas, com regimes sancionatórios que cada Estado deve estabelecer.

Sua aplicação ilustra um problema de sequência que convém registrar. A transposição aos ordenamentos nacionais avançou de forma desigual em relação ao prazo previsto e, como o código setorial se apoia em definições, autoridades e procedimentos que a diretiva cria, essa demora também retardou sua aplicação efetiva. Sem autoridade designada, sem equipe de resposta a incidentes operativa e sem capacidade de supervisão, o texto existe, mas não produz segurança.

Sobre esse patamar se ergue o Regulamento Delegado (UE) 2024/1366, em vigor desde junho de 2024, primeiro código de rede do setor elétrico europeu dedicado inteiramente à cibersegurança. Suas obrigações se organizam em torno de um sistema de gestão de cibersegurança, equivalente setorial de um sistema de gestão de segurança da informação, de dois conjuntos de controles, mínimos e avançados, cuja aplicação depende do nível de impacto da entidade. A isso se somam requisitos específicos de cadeia de suprimentos, gestão de crises, exercícios periódicos e verificação de cumprimento.

O ciclo de gestão de risco é trienal e está articulado em quatro níveis. Uma avaliação de alcance europeu identifica os processos críticos do sistema e define a escala comum de impacto; avaliações regionais agregam as informações de vários Estados; avaliações nacionais ficam a cargo

das autoridades competentes; cada entidade avalia seu próprio perímetro utilizando a matriz de impacto comum. Dentro dos doze meses seguintes à sua designação e depois a cada três anos, cada entidade deve reportar à sua autoridade os controles selecionados, o risco residual estimado e a lista de fornecedores críticos de tecnologia que intervêm em processos de impacto crítico.

A governança é tão relevante quanto o conteúdo. As metodologias e os controles não são ditados pela autoridade de forma unilateral: são desenvolvidos pelos operadores de transmissão em cooperação com a entidade europeia de operadores de distribuição, com participação da agência de reguladores de energia e da agência europeia de cibersegurança. A distribuição, como segmento, tem um assento formal na mesa onde se define o que lhe será exigido.

Os controles de cadeia de suprimentos merecem menção à parte por sua lógica. Não se pede à distribuidora que resolva o problema dos equipamentos já instalados: mudam-se as condições do que pode ser adquirido daqui em diante. Exigem-se princípios de segurança desde o design, arquiteturas de confiança zero[10], restrições de acesso, verificação de antecedentes do pessoal do fornecedor onde a legislação o permite, direitos contratuais de auditoria, rastreabilidade dos requisitos ao longo do ciclo de vida do produto e consideração explícita do risco de dependência de um único fornecedor. As obrigações se tornam vinculantes para os processos de compra iniciados seis meses após a adoção dos controles, as entidades de impacto crítico devem ainda verificar os componentes críticos mediante certificação ou mecanismos internos de garantia.

Alcance por criticidade: entidades designadas e perímetros de aplicação

Nenhuma entidade europeia fica coberta automaticamente pelo código. A autoridade nacional designa entidades de alto impacto e de impacto crítico, aplicando limiares derivados de um índice que avalia o efeito, nos fluxos elétricos transfronteiriços, do comprometimento dos processos operados por essa entidade. Os limiares provisórios, publicados pela rede europeia de operadores de transmissão junto com a entidade de operadores de distribuição, são expressos país a país em megawatts e variam consideravelmente conforme o porte e o grau de interconexão de cada sistema nacional.

A classificação não para na entidade. Dentro de cada empresa designada, delimitam-se perímetros: os ativos necessários para executar processos de alto impacto formam um perímetro sujeito aos controles mínimos e os necessários para processos de impacto crítico formam um perímetro sujeito aos controles avançados. A obrigação se dirige assim ao conjunto de ativos que produz o dano e não à totalidade da infraestrutura da empresa, o que limita o custo de cumprimento sem reduzir a proteção onde ela importa.

O mecanismo separa a exigência do porte da empresa e a vincula ao dano que sua falha causaria: uma distribuidora pequena cuja operação seja determinante para um processo crítico fica dentro do perímetro exigível, enquanto uma empresa maior situada em uma área amplamente redundante pode ficar em um nível inferior. O regulamento prevê ainda derrogações limitadas para os casos em que o custo de um controle seja desproporcional e existam salvaguardas alternativas.

Verificação do cumprimento e avaliação comparada do custo

A verificação é estruturada em ciclos.

[10] Confiança zero: Modelo de segurança que não presume como confiável nenhum equipamento, usuário ou conexão pelo simples fato de estar dentro da rede, exigindo verificação de identidade e permissões em cada acesso.

Cada entidade designada deve cobrir o alcance completo de verificação ao menos uma vez a cada três anos, com auditorias parciais anuais, pode atestar cumprimento mediante um esquema nacional de verificação supervisionado pela autoridade ou mediante auditoria independente de terceiro, com requisitos de independência, conhecimento setorial e confidencialidade. As entidades de impacto crítico devem demonstrar o cumprimento dos controles dentro dos vinte e quatro meses seguintes à sua adoção ou atualização.

Sobre o custo, o código encomenda aos reguladores nacionais de energia uma tarefa inédita: avaliar de forma comparada se os investimentos em cibersegurança das entidades reguladas são eficazes, eficientes e estão integrados aos processos de compra. Para isso, a agência europeia de reguladores publicou, em junho de 2025, um guia metodológico não vinculante e os reguladores nacionais devem realizar o exercício dentro dos doze meses seguintes. Os resultados são confidenciais e compartilhados entre as autoridades competentes, a agência de reguladores, a agência de cibersegurança e a Comissão.

O exercício não constitui reconhecimento tarifário. Seu efeito é prévio e de outra natureza: obriga o regulador a tratar o custo da cibersegurança como uma categoria própria, mensurável e comparável entre empresas, em vez de deixá-lo diluído dentro do gasto geral de tecnologia.

5.3. REINO UNIDO: O REGULADOR DE ENERGIA COMO AUTORIDADE DE CIBERSEGURANÇA

O Reino Unido combina dois traços que raramente coincidem: um regime de cibersegurança para infraestrutura crítica e um marco de regulação econômica por incentivos, ambos administrados pelo mesmo organismo no segmento de distribuição. O marco econômico é o RIIO, receitas determinadas por incentivos, inovação e resultados, um controle tarifário plurianual sob o qual os quatorze operadores de rede de distribuição apresentam planos de negócio que o regulador avalia, aprova e traduz em receitas permitidas, com mecanismos de ajuste durante o período. O regime de cibersegurança provém da normativa de segurança de redes e sistemas de informação de 2018, que o país manteve após sua saída da União Europeia e que atribui a cada setor uma autoridade competente própria. A autoridade técnica nacional em cibersegurança fornece o marco de avaliação e a doutrina, mas não fiscaliza diretamente as empresas do setor energético.

Uma autoridade única e um marco de avaliação por resultados

Para o segmento a jusante de gás e eletricidade, que inclui de forma explícita as distribuidoras, a autoridade competente é o próprio regulador de energia, em exercício conjunto com o ministério do setor. O mesmo organismo que fixa a remuneração da rede supervisiona sua cibersegurança, de modo que a exigência e seu financiamento são discutidos na mesma mesa, com o mesmo expediente e sob o mesmo critério de razoabilidade.

A avaliação se apoia no marco de avaliação cibernética desenvolvido pela autoridade técnica nacional, organizado em quatro objetivos, gerir o risco de segurança, proteger contra ataques, detectar os eventos de segurança e minimizar o impacto dos incidentes, catorze princípios e algo mais de quarenta resultados contribuintes. Cada resultado é acompanhado de indicadores de boa prática que descrevem a evidência que sustenta uma qualificação de alcançado, parcialmente alcançado ou não alcançado.

A diferença em relação a uma lista de verificação é substantiva: o marco especifica o que deve ser alcançado e não o que deve ser instalado. Isso desloca a discussão do inventário de ferramentas para a efetividade e permite que uma empresa pequena alcance um resultado com uma arquitetura simples e bem operada sem replicar a

infraestrutura de um grande grupo. O regulador de energia adapta o marco mediante um perfil setorial que define o nível esperado segundo o tipo de entidade e tem endurecido áreas específicas, em particular a segurança da cadeia de suprimentos e as exigências sobre fornecedores críticos.

RIIO: a cibersegurança como rubrica tarifária

O controle tarifário vigente para a distribuição elétrica, que rege de abril de 2023 a março de 2028, separa a cibersegurança do plano de negócios ordinário e lhe atribui tratamento próprio.

O design tem quatro peças. Primeiro, as empresas apresentam planos de resiliência cibernética diferenciados para tecnologia da informação e para tecnologia de operação, avaliados com base em requisitos mínimos de qualidade: o financiamento é vinculado a um plano verificável e não a uma declaração de intenções. Segundo, esse plano recebe uma alocação específica dentro das receitas permitidas. Terceiro, existem mecanismos de reabertura, um para tecnologia da informação e outro para tecnologia de operação, que permitem ajustar a alocação durante o período tarifário quando as circunstâncias mudam, com um prazo de resolução limitado para que a decisão seja incorporada ao processo anual de atualização de receitas. Quarto, a alocação opera como um produto do controle tarifário sujeito à condição de uso ou devolução: o dinheiro reconhecido para cibersegurança não pode ser destinado a outra finalidade e, se o plano comprometido não for executado, é devolvido.

O resultado é um arranjo simétrico. O regulador financia, mas exige um plano verificável, reserva-se a revisão periódica e impede que a rubrica se converta em folga orçamentária. A reabertura reconhece ainda de forma explícita que a ameaça evolui mais rápido do que o ciclo regulatório, um descompasso que nenhum controle tarifário de período fixo pode resolver por via da previsão.

O regime de segurança, por sua vez, está em revisão: em novembro de 2025 foi apresentado ao Parlamento um projeto de lei de cibersegurança e resiliência que atualiza a normativa de 2018 e amplia as obrigações existentes, entre outras matérias sobre fornecedores e prestadores de serviços gerenciados.

5.4. AUSTRÁLIA: A PROPORCIONALIDADE COMO PRINCÍPIO DE DESIGN

A Austrália construiu seu regime sobre duas peças que operam em planos distintos: uma lei transversal de infraestrutura crítica, aplicável a um amplo conjunto de setores, e um marco de maturidade específico do setor energético desenvolvido pela própria indústria junto com o operador do mercado e as agências de governo.

O operador do mercado ocupa uma posição singular. Além de administrar o mercado atacadista e operar o sistema, atua como coordenador da cibersegurança setorial: convoca o exercício anual de avaliação, consolida os resultados e publica o marco e seus materiais de orientação. Essa dupla condição explica que o instrumento tenha sido desenvolvido de dentro do setor e não como uma imposição externa e que, em seus primeiros anos, tenha sido inteiramente voluntário.

O AESCSF: um modelo de maturidade setorial

O marco de cibersegurança do setor energético australiano foi publicado pela primeira vez em 2018 e atualizado em 2022. Foi construído sobre modelos de capacidade e marcos de referência internacionais já existentes, principalmente o modelo de maturidade de capacidades do subsetor elétrico do Departamento de Energia norte-americano e o marco de cibersegurança do instituto nacional de padrões, remete a

padrões de controle de uso geral para o detalhe técnico.

A avaliação é organizada em onze domínios: gestão do risco; gestão de ativos, mudanças e configuração; gestão de identidades e acessos; gestão de ameaças e vulnerabilidades; consciência situacional; intercâmbio de informações e comunicações; resposta a eventos e incidentes e continuidade da operação; gestão da cadeia de suprimentos e das dependências; gestão da força de trabalho; gestão do programa de cibersegurança e; gestão da privacidade conforme a legislação australiana. Dentro de cada domínio, as práticas são ordenadas em níveis de maturidade que vão de zero a três.

Sobre essa base definem-se perfis de segurança acumulativos. Cada perfil superior pressupõe ter alcançado o anterior, o perfil objetivo de cada organização depende de sua criticidade para o setor e não de seu faturamento nem de seu número de consumidores. Uma empresa pequena não fica isenta: fica situada em um perfil inferior, com um objetivo alcançável e uma trajetória comparável com a das demais. Todas usam o mesmo idioma, o mesmo instrumento de medição e a mesma escala, o que torna os resultados agregáveis e comparáveis entre organizações e ao longo do tempo.

Esse último traço explica a origem do marco. Nasceu como ferramenta de autoavaliação setorial e durante vários anos o setor se mediu a si mesmo, em um ciclo anual coordenado pelo operador do mercado, antes que a lei lhe exigisse qualquer coisa. A medição produziu a linha de base que depois permitiu fixar obrigações com níveis e datas realistas.

Convém destacar a existência de um domínio específico dedicado à gestão da força de trabalho, que converte a disponibilidade de pessoal qualificado em uma dimensão medida e comparável, não em uma restrição implícita que cada empresa administra por conta própria.

De marco voluntário a obrigação legal: a lei de infraestrutura crítica

A lei australiana de segurança de infraestrutura crítica e suas regras de programa de gestão de riscos tornaram obrigatório, desde agosto de 2024, que as entidades responsáveis adotem um marco de cibersegurança reconhecido; o marco setorial energético foi admitido como um deles, ao lado de padrões internacionais de uso geral.

O regime foi substancialmente endurecido em junho de 2026, quando entraram em vigor regras reforçadas que exigem das entidades responsáveis do setor energético alcançar o segundo perfil de segurança do marco setorial até 30 de junho de 2028, com prazos de implementação de doze a vinte e quatro meses para os demais requisitos e com a exigência alinhada ao ciclo anual de atestação já existente. A obrigação legal não enumera controles: fixa um nível de maturidade e uma data.

O resultado é um modelo de duas camadas. A lei geral obriga a contar com um marco reconhecido e a alcançar um determinado nível em um prazo determinado; o marco setorial, elaborado com a indústria e atualizado com ela, define como esse nível é mensurado. O legislador não precisa escrever controles técnicos que envelhecerão em poucos anos e a discussão com o setor não versa sobre se ele cumpre, mas sobre como demonstra que cumpre.

A articulação com a regulação econômica ocorre por uma via menos estruturada do que a britânica, mas igualmente operativa: as distribuidoras apresentam ao regulador econômico casos de negócio específicos para alcançar determinados níveis de maturidade do marco setorial. Quando a obrigação está expressa como um nível verificável com data certa, o custo de alcançá-la torna-se argumentável dentro do processo tarifário.

5.5. ONTÁRIO: REGULAÇÃO DE MATURIDADE PARA DISTRIBUIDORAS HETEROGÊNEAS

O caso de Ontário interessa pela composição de seu universo regulado. O regulador de energia provincial supervisiona cerca de sessenta distribuidoras locais, em sua maioria de titularidade municipal e de escalas muito díspares, que vão de empresas que atendem a mais de um milhão de consumidores até companhias municipais de poucos milhares. É uma estrutura de setor que se assemelha mais à de vários países latino-americanos do que à de qualquer outro dos referenciais revisados.

O instrumento normativo também é particular. O regulador não recorreu a uma lei: incorporou as obrigações de cibersegurança mediante emendas aos códigos de transmissão e de distribuição, que são regulamentos de sua própria competência e fazem parte das condições da licença. Isso lhe permitiu agir com rapidez e ajustar a abordagem ao longo do tempo sem abrir um processo legislativo.

Em 2018, essas emendas obrigaram os transmissores e distribuidores licenciados a utilizar um marco de cibersegurança desenvolvido com a indústria e a informar ao regulador o nível de maturidade alcançado. O marco se apoiou em um modelo de capacidade público de amplo uso, com níveis de maturidade aplicados sobre as funções de identificar, proteger, detectar, responder e recuperar, incorporou ainda uma dimensão de privacidade.

O mecanismo de reporte é seu traço mais distintivo: uma autocertificação anual do nível de maturidade alcançado, assinada pelo máximo executivo da empresa e apresentada ao regulador. Isso não exige que a autoridade monte um corpo de inspetores especializados em segurança industrial, uma capacidade cara, escassa e difícil de reter em qualquer administração pública, produz um efeito que nenhuma auditoria externa consegue com a mesma economia: obriga a que o assunto chegue ao mais alto nível de decisão da empresa ao menos uma vez por ano, com uma assinatura pessoal em jogo.

Em outubro de 2024, entrou em vigor um padrão de cibersegurança obrigatório que substitui a abordagem declaratória por requisitos exigíveis. A sequência completa, seis anos de medição e reporte antes da obrigação, não foi uma demora, mas a construção das duas condições que tornam viável uma norma obrigatória: que o regulador saiba onde realmente está seu setor e que as empresas disponham de uma linha de base própria a partir da qual planejar.

5.6. ÍNDIA: REGULAÇÃO EM UM SISTEMA DE GRANDE ESCALA E MATURIDADE DESIGUAL

A Índia regula o maior sistema elétrico do mundo por número de conexões, com distribuidoras estaduais, privadas e mistas de desempenho financeiro e técnico muito desigual. A autoridade central de eletricidade, organismo técnico do governo federal, tem competência para editar normas aplicáveis a todo o setor e utilizou essa prerrogativa para instalar obrigações de cibersegurança sem aguardar que as empresas alcançassem um nível homogêneo de maturidade.

O percurso foi do menor para o maior nível de exigibilidade. A autoridade emitiu primeiro guias de cibersegurança para o setor elétrico e avançou em seguida para um regulamento setorial, cujo esboço foi submetido a consulta pública em outubro de 2025. O alcance proposto cobre geração, transmissão e distribuição e se estende às bolsas de energia, aos centros de despacho de carga e aos fornecedores de sistemas de informação e controle, de modo que a obrigação não para na empresa regulada, mas alcança quem lhe fornece a tecnologia com que opera.

As obrigações são marcadamente prescritivas em matéria de governança, em con-

traste com a abordagem de resultados britânica e com a de maturidade australiana: designação de um responsável de segurança da informação e de um suplente, ambos da alta direção e com reporte ao mais alto nível da organização; uma divisão de segurança da informação com operação permanente; auditorias obrigatórias por auditores credenciados e; requisitos sobre a cadeia de suprimentos de sistemas de controle.

O componente institucional é o mais singular do caso. A Índia conta com uma equipe de resposta a incidentes específica do setor elétrico, que atua como agência central de reporte, resposta e análise e se articula com a equipe nacional. A existência desse ponto único converte a notificação obrigatória em um intercâmbio: a empresa que informa recebe em troca alertas, análise e coordenação, a autoridade acumula uma visão agregada da ameaça que nenhuma empresa individual poderia construir por conta própria.

5.7. MECANISMOS QUE A EXPERIÊNCIA INTERNACIONAL COLOCA SOBRE A MESA

Os seis casos anteriores admitem uma leitura transversal, que organiza a experiência não por jurisdição, mas pelo problema de design que cada instrumento resolve.

Alcance: como se define quem fica dentro

Observam-se quatro critérios de inclusão. O primeiro é o impacto sobre o sistema, medido com um índice comum e expresso em limiares por país, como na União Europeia: é o mais preciso e o mais exigente em informação. O segundo é a classificação de ativos por criticidade, como nos Estados Unidos: não define quais empresas ficam dentro, mas quais requisitos se aplicam a cada ativo. O terceiro combina segmento e número de consumidores regulados, é o critério que aparece nas normas setoriais mais recentes, inclusive na que está sendo elaborada no Chile. O quarto é a designação administrativa por classe de ativo crítico, como na Austrália. A eles se soma, em Ontário, a via mais simples de todas: a licença setorial, que incorpora sem exceções a totalidade do universo regulado.

Critério de inclusão	Onde se aplica	Cobre distribuição?	Exigência de informação para o regulador
Impacto sobre o sistema, com limiares por país	União Europeia	Sim, se superar o limiar	Alta: requer modelar impacto sistêmico por operador
Criticidade do ativo (alto / médio / baixo)	Estados Unidos	Apenas ativos do sistema atacadista	Média: inventário e classificação de ativos
Segmento e número de consumidores regulados	Índia; norma em elaboração no Chile	Sim, de forma explícita	Baixa: informação já disponível no regulador
Designação administrativa por classe de ativo crítico	Austrália	Sim	Média: definição legal de classes de ativos
Licença setorial (todos os licenciados)	Ontário	Sim, sem exceção de porte	Baixa: o universo é o cadastro de licenças

Tabela 5.1. Critérios de definição do universo obrigado e sua exigência de informação.

Exigência: controle prescritivo, sistema de gestão ou maturidade avaliada

Os três modelos coexistem e não são excludentes. O controle prescritivo, o padrão que enumera o que deve estar implementado, se audita melhor do que qualquer outro, mas envelhece rapida-

mente e penaliza desproporcionalmente as empresas menores, que devem implementar o mesmo com menos recursos. O sistema de gestão transfere o ônus da prova para a empresa e se adapta a diferentes portes, mas corre o risco de se converter em cumprimento documental. A maturidade avaliada acompanha uma trajetória em vez de fixar um limiar binário, é a que melhor se adapta a um setor heterogêneo e também a que mais exige do regulador, porque avaliar maturidade requer julgamento técnico e não apenas verificação.

As jurisdições mais avançadas os combinam. O Reino Unido avalia por resultados e financia um plano. A Austrália sobrepõe uma lei que obriga a alcançar um nível e um marco setorial que define como se mede. A União Europeia exige um sistema de gestão com controles diferenciados por nível de impacto e verificação periódica. A combinação, mais do que a escolha entre modelos, é o que caracteriza os marcos maduros.

Financiamento: quem paga e com qual instrumento

Este é o ponto onde a experiência internacional é mais escassa. Identificam-se quatro instrumentos, do maior para o menor grau de complexidade institucional:



Fig. 5. Como se financia a cibersegurança: quatro instrumentos internacionais

1. Partida tarifária específica, com reabertura e condição de uso ou perda (Reino Unido). É o desenho mais completo. Requer um controle tarifário plurianual, com mecanismos de ajuste dentro do período.

2. Ativo regulatório com diferimento e retorno (Estados Unidos). Sua falta de uso é um alerta sobre a calibragem: o benefício precisa superar com folga o custo de solicitálo.

3. Avaliação comparada da eficiência dos investimentos (União Europeia). É o passo mais barato e o único que não exige modificar o marco tarifário: apenas obriga a medir o custo da cibersegurança como categoria separada e a comparálo entre empresas.

4. Caso de negócio perante o regulador econômico (Austrália). Funciona onde o marco tarifário já admite a apresentação de planos de investimento discutíveis, e se apoia no fato de que a obrigação esteja expressa como um nível verificável e com data definida.

A observação mais importante é que nenhum desses quatro instrumentos faz parte da norma de segurança: todos se desenvolvem na regulação econômica. A norma setorial define o que deve ser feito; o marco de remuneração define se é possível fazê-lo.

Proporcionalidade: como a cooperativa convive com o grande grupo

Todas as jurisdições revisadas resolveram esse problema mediante instrumentos de graduação e nenhuma o fez isentando as empresas menores.

Técnica	Jurisdição	Como se determina o nível	O que se exige da empresa menor
Limiares de impacto sobre o sistema	União Europeia	Índice comum de impacto, com limiares nacionais em MW	Nada, se estiver abaixo do limiar; controles mínimos completos, se o superar
Níveis de impacto do ativo	Estados Unidos	Classificação do sistema cibernético em alto, médio ou baixo	Requisitos reduzidos, proporcionais ao ativo que opera
Perfis de segurança acumulativos	Austrália	Criticidade da entidade para o setor	Alcançar o primeiro perfil, com data certa e trajetória definida
Perfil setorial do marco de avaliação	Reino Unido	Tipo de entidade, definido pelo regulador de energia	Demonstrar resultados de segurança, não implementar controles idênticos
Níveis de maturidade autocertificados	Ontário	Autoavaliação anual sobre o marco comum	Declarar seu nível real e seu plano de melhoria, assinado pelo máximo executivo
Prazos diferenciados	Todas	Criticidade do ativo ou do tipo de entidade	Mais tempo para alcançar o mesmo objetivo

Tabela 5.2. Técnicas de proporcionalidade observadas na experiência internacional.

Convém destacar a última linha. Todas as jurisdições usam o tempo como instrumento de proporcionalidade: prazos de trinta e seis e sessenta meses conforme a criticidade do ativo nos Estados Unidos; doze e vinte e quatro meses conforme o nível de impacto na União Europeia; janelas de doze a vinte e quatro meses e uma meta setorial fixada para 2028 na Austrália. Diferenciar prazos não requer nenhuma sofisticação metodológica e produz boa parte do efeito de proporcionalidade que se busca.

Notificação de incidentes e resposta coordenada

Todas as jurisdições revisadas têm notificação obrigatória de incidentes com prazos curtos e todas a acompanham de dois elementos: um canal setorial de resposta e análise e regras explícitas de confidencialidade e de anonimização das informações compartilhadas. A notificação sem proteção de quem notifica produz menos notificações, não menos incidentes.

Um detalhe do caso norte-americano ilumina o ponto por outro ângulo. Dos dois únicos conceitos incluídos na lista de investimentos pré-aprovados para o incentivo tarifário, um é a participação no programa de intercâmbio de informações sobre ameaças. Ou seja, a jurisdição que mais sanciona o descumprimento decidiu também financiar a participação no mecanismo de informação compartilhada.

5.8. LEITURAS PARA A AMÉRICA LATINA

A comparação anterior deixa uma assimetria que convém enunciar antes de qualquer transferência. A experiência internacional oferece respostas abundantes e comprovadas sobre o que exigir e, como graduar a exigência, além de respostas escassas sobre como financiá-la. As duas mais completas, a britânica e a norte-americana, não provêm de normas de segurança, mas de marcos de regulação econômica, e a segunda, além disso, ainda não chegou a ser utilizada.

Três condições que os referenciais dão por pressupostas não estão garantidas na região. A primeira é um regulador com capacidade técnica própria ou com acesso estável a ela, para avaliar maturidade em segurança industrial: sem essa capacidade, qualquer norma se degrada a verificação documental. A segunda é uma agência nacional de cibersegurança operativa, com equipe de resposta a incidentes, que receba as notificações e devolva análise e coordenação; sem ela, a notificação obrigatória é um ônus sem contrapartida. A terceira é um marco tarifário com revisões periódicas e espaço para rubricas novas: sem ela, a discussão sobre financiamento não tem onde ocorrer. Reconhecer essas condições não invalida a transferência dos mecanismos; define sua sequência.

Com essa ressalva, seis elementos da experiência internacional são aplicáveis no curto prazo e com baixo custo regulatório:

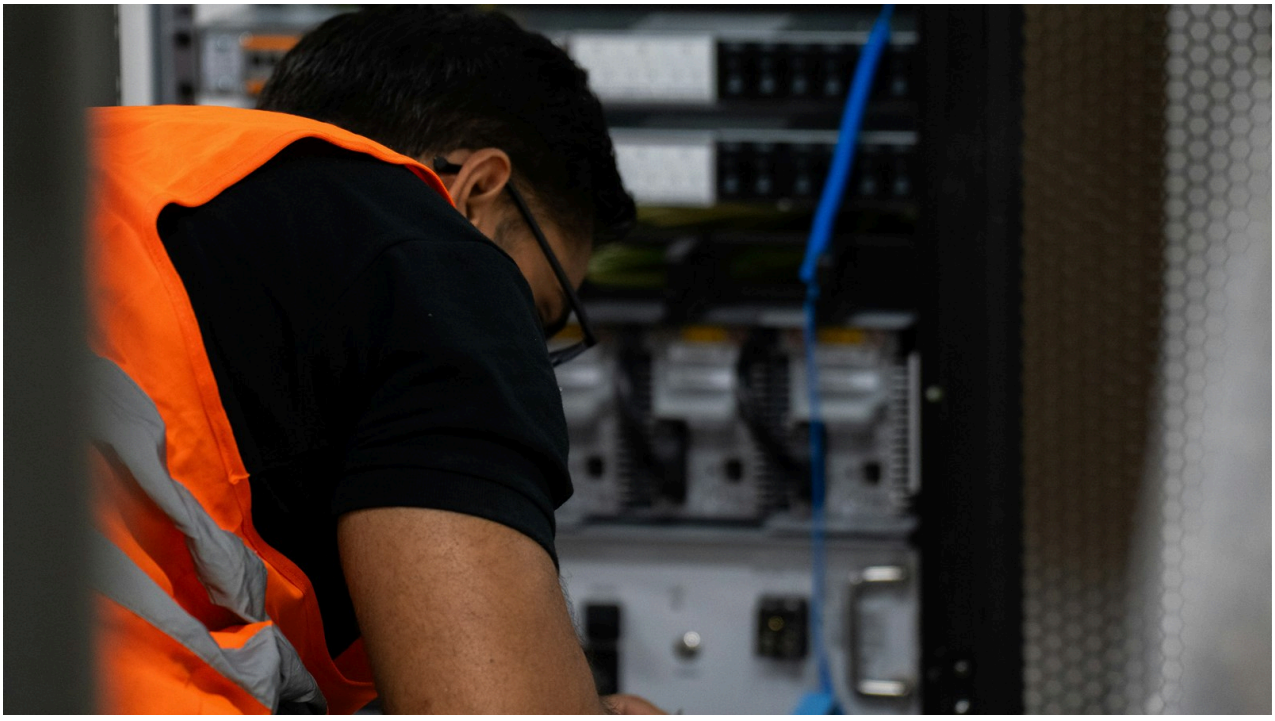
1. **Medir antes de exigir.** Austrália e Ontário construíram seus regimes obrigatórios com base em vários anos de medição prévia, e foi essa medição que permitiu, depois, fixar níveis e datas realistas. O benchmarking que sustenta este documento é exatamente esse primeiro passo; sua continuidade periódica é o investimento regulatório mais barato disponível.
2. **Adotar um marco de maturidade como linguagem setorial comum.** Não é necessário criar um novo: os marcos australiano, canadense e britânico são públicos e se apoiam em modelos de capacidade de uso livre. O que pode ser transferido é a decisão de adotar um deles como referência — e isso é também o que torna comparáveis os resultados entre empresas e entre países.
3. **A autocertificação anual assinada pelo principal executivo.** É o mecanismo com melhor relação entre custo regulatório e efeito de governança em todo o repertório revisado, e não exige construir capacidade de fiscalização técnica.
4. **Separar a norma habilitante do padrão setorial.** Isso permite que a norma obrigue a alcançar um nível em uma data específica, enquanto o detalhamento técnico pode ser atualizado pela indústria sem necessidade de reformar a norma.
5. **Transferir a cibersegurança para as condições de compra.** Exigir segurança desde o design, gestão de credenciais e direitos contratuais de auditoria nas novas aquisições evita o problema — financeiramente inviável — de intervir em uma frota já instalada.
6. **Medir o custo da cibersegurança como categoria separada.** É o passo prévio a qualquer discussão sobre reconhecimento tarifário; não exige modificar o marco de remuneração e pode começar com as informações que as empresas já produzem.

Outros três elementos, por outro lado, não são diretamente transferíveis. O modelo sancionatório norte-americano pressupõe um aparato de auditoria e fiscalização cuja construção levaria anos e cujo custo dificilmente se justifica para o segmento de distribuição. O índice europeu de impacto exige modelar o efeito sistêmico de cada operador sobre os fluxos do sistema, uma capacidade que hoje não está disponível

de forma generalizada; os critérios de alcance realistas no curto prazo são a classificação de ativos por criticidade e a combinação de segmento com número de consumidores regulados. O mecanismo tarifário britânico depende de um controle plurianual com reaberturas dentro do período: o que é transferível não é sua forma, mas seu princípio, ou seja, uma rubrica diferenciada, vinculada a um plano verificável, revisável durante o período e não fungível.

Resta por último uma decisão que a experiência internacional não resolve, porque admite duas respostas igualmente defensáveis. Austrália e Ontário mediram durante anos antes de exigir; a Índia regulou sem esperar maturidade, apostando que a obrigação gera a capacidade. A escolha entre um e outro não é técnica, mas política, depende da urgência percebida pelo regulador e de quanto acompanhamento está disposto a oferecer durante a transição. As recomendações do capítulo seguinte partem desse repertório.

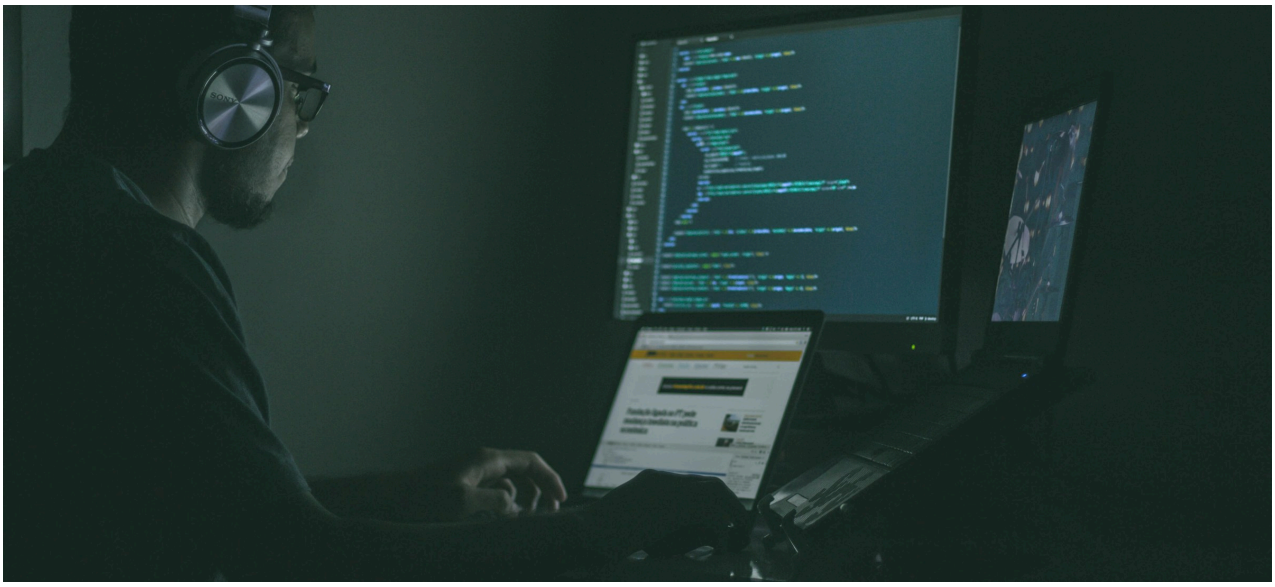
> Adotar um marco de maturidade como linguagem setorial comum.



06

CONCLUSÕES E RECOMENDAÇÕES REGULATÓRIAS

A transição energética que a regulação impulsiona é, na prática, uma transição digital, cada equipamento que se conecta à rede amplia a superfície que precisa ser protegida. A evidência reunida pelo benchmarking regional, com vinte e cinco distribuidoras de dez países, mostrou que o setor já está respondendo a essa exposição e que o faz com um padrão que se repetiu nas cinco dimensões examinadas: a infraestrutura de operação, a capacidade de detecção e resposta, os terceiros e os dados, as pessoas e a governança. Esse avanço, porém, não é homogêneo, a linha que o divide é econômica antes de ser técnica: avança-se onde a proteção toma a forma de investimento em ativos, o gasto de capital que os marcos tarifários sabem incorporar à base de remuneração; e fica para trás onde exige gasto operacional permanente, a vigilância diária, a verificação dos terceiros, a formação do pessoal e os especialistas que precisam ser retidos. A revisão da regulação latino-americana confirmou a outra metade do problema porque, nos onze marcos examinados, esse gasto não existe como categoria reconhecida na tarifa e as empresas precisam custeá-lo a partir de rubricas concebidas para outros fins. A experiência internacional, por sua vez, ensina que a exigência e seu financiamento constituem um único problema de design, porque onde a obrigação chegou sem uma via de custeio o cumprimento ficou estagnado; onde o incentivo foi mal calibrado, como o ativo regulatório norte-americano que nenhuma empresa solicitou, ficou escrito e sem uso e; onde ambos foram desenhados juntos, como a rubrica tarifária britânica condicionada a um plano verificável, a proteção deixou de competir por recursos com o restante do orçamento. Desse percurso se depreende que o problema de fundo não é técnico, mas de design regulatório e, que enquanto não for corrigido, o nível de proteção de cada rede continuará dependendo da convicção e da folga financeira de cada empresa. Reverter esse resultado não consiste em escolher entre exigir e financiar, mas em fazer as duas coisas em um mesmo design, porque uma obrigação sem via de custeio produz descumprimento e um custeio sem obrigação não garante proteção.



O design conjunto começa pela exigência. A experiência comparada mostra que em setores onde coexistem grandes grupos com milhões de consumidores e cooperativas rurais de economias muito distintas, uma norma severa e uniforme penaliza o menor e pode empurrá-lo a ficar fora do alcance da regra antes de que se proteja melhor. Os marcos que melhor resolveram essa heterogeneidade, o australiano, o britânico e o de Ontário, compartilham duas decisões: graduam a exigência conforme a criticidade de cada operação e não conforme o porte de cada empresa e separam a norma habilitante, que fixa o nível a alcançar e seu prazo, do padrão técnico que define como mensurá-lo, de modo que a empresa menor e a maior percorrem a mesma escala em ritmos distintos, mas verificáveis, o detalhe técnico se atualiza com a indústria sem necessidade de reformar a lei. O financiamento, por sua vez, deve ser definido como o conjunto de mecanismos para justificar, supervisionar e verificar os investimentos que efetivamente reduzem o risco operacional. O repertório internacional disponível avança do menor para o maior grau de complexidade institucional: medir o custo da cibersegurança como categoria separada, o que não exige modificar o marco tarifário e entrega ao regulador a informação de que hoje não dispõe; admitir casos de negócio perante o regulador econômico para alcançar níveis definidos de maturidade e; estabelecer uma rubrica tarifária específica condicionada a um plano verificável, com revisão periódica e devolução do não executado.

Há uma terceira frente que não exige reformas tarifárias, porque depende de decisões que o regulador pode tomar diretamente com seus próprios instrumentos: a infraestrutura comum de que depende toda defesa. A primeira peça é a notificação obrigatória de incidentes, cujo design importa tanto quanto sua existência, porque se notificar expõe automaticamente a uma sanção, o incentivo racional é ocultar. A notificação deve ser acompanhada de confidencialidade, de regras de anonimização e do princípio de que a notificação de boa-fé não constitui por si só prova de negligência, um princípio que a legislação equatoriana de 2026 já incorporou e que mostra que a região está em condições de adotá-lo. A segunda peça é a resposta coordenada. Um ataque bem-sucedido contra uma distribuidora não é um problema individual, porque a interdependência do ecossistema elétrico permite que o comprometimento de um elo se propague pela cadeia. Diante de ameaças que operam em escala transnacional, o intercâmbio de informações e uma equipe de resposta setorial elevam a capacidade de todas as empresas sem que cada uma precise construí-los separadamente e, esse espaço está hoje quase vazio na região, com apenas um CSIRT elétrico formalizado. A terceira peça volta à origem do problema, porque os mesmos planos de medição inteligente, telecontrole e automação que os reguladores impulsionam e aprovam podem incorporar a segurança como requisito de design, nas condições de compra e na aprovação dos projetos, de modo que a modernização não continue ampliando a superfície exposta mais rapidamente do que se protege.

As empresas, por sua vez, não precisam aguardar a regulação para avançar, o próprio diagnóstico mostra que já começaram. Medir-se periodicamente é a primeira tarefa, porque os regimes de maturidade que operam no mundo foram construídos sobre anos de medição setorial prévia e esse caminho já está iniciado na região com exercícios como o que sustenta este diagnóstico. O que vem a seguir é adotar um marco de maturidade público como linguagem comum, que permite a cada empresa fixar um nível objetivo e demonstrar seu avanço; levar a cibersegurança para a governança corporativa, com um responsável com acesso direto à alta administração, uma rubrica orçamentária própria e o risco expresso em termos econômicos, que é o idioma em que os

conselhos decidem; assegurar contratualmente cada nova aquisição, exigindo segurança desde o design e direitos de auditoria, para que a frota instalada hoje não repita as vulnerabilidades da instalada ontem e; enfrentar coletivamente a escassez de talentos especializados, que é do mercado e não de cada empresa. Nada disso substitui a tarefa do regulador, mas a facilita, porque um setor que se mede, se governa e demonstra seus avanços torna verificável o gasto que pede reconhecimento. Em última análise, a decisão pendente é um cálculo simples: regular e financiar a proteção das redes custa menos hoje do que o incidente que essa proteção evita e, o custo de postergá-la não desaparece, acumula-se em silêncio e termina sendo pago pelo consumidor, como interrupção do serviço, como vazamento de seus dados ou como gasto de emergência.



Fig. 6. Recomendações segundo a complexidade de implementação

07
REFERÊNCIAS

Adaptix Networks. (2022, 8 de julho). *Filtran datos personales de clientes CFE*. https://www.adaptixnetworks.com/filtran-datos-personales-de-clientes-cfe/

Agência Nacional de Energia Elétrica. (2021). *Resolução Normativa n.º 964, de 14 de dezembro de 2021: estabelece a Política de Segurança Cibernética e os requisitos mínimos de segurança cibernética para os agentes do setor elétrico*. https://www2.aneel.gov.br/cedoc/ren2021964.html

Agência Nacional de Energia Elétrica. (2025). *Despacho n.º 427, de 17 de fevereiro de 2025: fixa cronograma de envio periódico de dados de maturidade e riscos de segurança cibernética pelos agentes do setor elétrico*. https://www2.aneel.gov.br/cedoc/dsp2025427.pdf

Argentina. (2000). *Ley 25.326: Ley de protección de datos personales*. Agencia de Acceso a la Información Pública.

Argentina. (2017). *Decreto 577/2017: Comité de Ciberseguridad*. Boletín Oficial. https://www.argentina.gob.ar/normativa/nacional/decreto-577-2017-277518/actualizacion

Argentina. (2021). *Decisión Administrativa 641/2021: requisitos mínimos de seguridad de la información para organismos del sector público nacional*. Boletín Oficial. https://www.boletinoficial.gob.ar/detalleAviso/primera/246104/20210628

Argentina. (2025). *Decreto 941/2025: creación del Centro Nacional de Ciberseguridad*. InfoLeg. https://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=422011

Asamblea Legislativa de El Salvador. (2025, 30 de abril). *Transferencia de recursos permitirá funcionar la Agencia de Ciberseguridad del Estado*. https://www.asamblea.gob.sv/node/13555

Biblioteca del Congreso Nacional de Chile. (s.d.). *LeyChile* [Base de dados normativa]. https://www.bcn.cl/leychile/

Bolívia. (1997). *Código Penal, capítulo XI: delitos informáticos*. https://www.minsalud.gob.bo/images/Documentacion/normativa/LEY%201768%20CODIGO%20PENAL.pdf

Bolívia. (2013). *Decreto Supremo n.º 1793: reglamento de la Ley n.º 164*. https://www.oopp.gob.bo/wp-content/uploads/2021/07/2013-DS1793-Reglamento-Ley-164.pdf

Centro Nacional de Ciberseguridad. (2026). *Disposición 1/2026: reglamento técnico sobre planes de contingencia y centros de procesamiento de datos alternativos*. https://www.argentina.gob.ar/normativa/nacional/disposici%C3%B3n-1-2026-425749/texto

CERT-PY. (2025). *Marco legal: Decreto n.º 3900/2025 e Resolución MITIC n.º 259/2025*. https://www.cert.gov.py/marco-legal/

CERT-UA. (2022, 12 de abril). *Ciberataque do grupo Sandworm (UAC-0082) contra instalações energéticas da Ucrânia mediante os programas maliciosos INDUSTROYER2 e CADDYWIPER* (CERT-UA#4435). https://cert.gov.ua/article/39518

Cherepanov, A. (2017). *Win32/Industroyer: a new threat for industrial control systems* [Relatório técnico]. ESET. https://web-assets.esetstatic.com/wls/2017/06/Win32_Industroyer.pdf

Chile. (2024). *Ley n.º 21.663: Ley marco de ciberseguridad e infraestructura crítica de la información*. Biblioteca del Congreso Nacional. https://www.bcn.cl/leychile/navegar?idNorma=1202434

Chile. (2024). *Ley n.º 21.719: regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales*. Biblioteca del Congreso Nacional. https://www.bcn.cl/leychile/navegar?idNorma=1209272

Chile, Ministerio del Interior y Seguridad Pública. (2024). *Decreto Supremo n.º 295: reglamento sobre notificación de incidentes de ciberseguridad de la Ley 21.663* [Alerta precoce em 3 horas; relatório ou atualização em 72 horas, ou 24 horas para operadores de importância vital com serviço afetado; relatório final em 15 dias]. Biblioteca del Congreso Nacional. https://www.bcn.cl/leychile/Navegar?idNorma=1211466

Comisión de Regulación de Energía y Gas. (2022). *Resolución CREG 101 001 de 2022: medición avanzada (AMI), ciberseguridad e ISO/IEC 27001*. Gestor Normativo de la CREG. https://gestornormativo.creg.gov.co/gestor/entorno/docs/resolucion_creg_101-1_2022.htm

Comisión de Regulación de Energía y Gas. (2022). *Resolución CREG 701 11 de 2022: fundamentación sobre la prohibición de traslado tarifario de medidores (art. 56 de la Ley 2099/2021)*. Gestor Normativo de la CREG. https://gestornormativo.creg.gov.co/gestor/entorno/docs/resolucion_creg_701-11_2022.htm

Congreso de la República de Guatemala. (s.d.). *Iniciativa de Ley n.º 6347: Ley de ciberseguridad*. https://www.congreso.gob.gt/assets/uploads/info_legislativo/iniciativas/ea912-6347.pdf

Congreso de la República de Guatemala, Comisión de Asuntos de Seguridad Nacional. (2025). *Dictamen 01-2025 sobre la Iniciativa de Ley n.º 6347*. https://www.congreso.gob.gt/assets/uploads/comisiones/dictamenes/97fef-dictamen-6347-fav-casn.pdf

Conselho Nacional de Operação. (s.d.). *Acordo CNO 2088: procedimento e formato de notificação de incidentes, CSIRT setorial elétrico e MISP*. https://www.cno.org.co/content/acuerdo-2088-por-el-cual-se-aprueba-el-procedimiento-y-formato-de-reporte-de-incidentes

Conselho Nacional de Operação. (s.d.). *Acordos* [Compilação: 788/2015, 1241/2019, 1347/2020, 1463/2021 e 1502/2021]. https://www.cno.org.co/calendar-acuerdos

Conselho Nacional de Operação. (s.d.). *Cibersegurança* [Página institucional do comitê de cibersegurança]. https://www.cno.org.co/content/ciberseguridad-7

Conselho Nacional de Operação. (2025). *Acordo CNO 1960 de 2025: atualização do Guia de cibersegurança com abordagem baseada em risco*. https://www.cno.org.co/content/acuerdo-1960-por-el-cual-se-aprueba-la-actualizacion-de-la-guia-de-ciberseguridad-y-se

Diario Oficial de El Salvador. (2024, 15 de novembro). *Decretos n.º 143 e n.º 144*. https://transparencia.mh.gob.sv/downloads/pdf/700-UAIP-LY-2024-14993.pdf

Dragos. (2025). *OT/ICS cybersecurity report: a year in review* (8.ª ed.). https://hub.dragos.com/ot-cybersecurity-year-in-review-2025

El Deber. (2026, 14 de janeiro). *El Gobierno reordena la firma digital y saca a la ADSIB de la Vicepresidencia*. https://eldeber.com.bo/pais/gobierno-reordena-firma-digital-saca-adsib-vicepresidencia_1768399727

El Salvador. (2024). *Decreto Legislativo n.º 143: Ley de ciberseguridad y seguridad de la información*. Refworld. https://www.refworld.org/es/leg/legis/pleg/2024/149335

ESET Research. (2022, 12 de abril). *Industroyer2: Industroyer reloaded*. WeLiveSecurity. https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

FUNDESA. (s.d.). *Ley de ciberseguridad debería regresar a la Comisión*. https://fundesa.org.gt/en/publications/opinion/ley-de-ciberseguridad-deberia-regresar-a-la-comision

Gobierno de Colombia. (2022). *Decreto 338 de 2022: cria o colCERT, o CSIRT Gobierno, o CSIRT Defensa e a Plataforma Nacional de Notificação e Acompanhamento de Incidentes*. https://normograma.mintic.gov.co/mintic/compilacion/docs/decreto_0338_2022.htm

InfoLeg. (s.d.). *Compilado de normativa de ciberseguridad*. https://servicios.infoleg.gob.ar/infolegInternet/anexos/365000-369999/365238/norma.htm

La República. (2022, 22 de agosto). *Ley de ciberseguridad*. https://www.larepublica.net/noticia/ley-de-ciberseguridad

La Tercera. (2019). *Gobierno argentino cree que apagón no fue un ciberataque pero no lo descarta*. https://www.latercera.com/mundo/noticia/gobierno-argentino-cree-apagon-no-fue-ciberataque-no-lo-descarta/702370/

Lee, R. M., Assante, M. J. e Conway, T. (2016). *Analysis of the cyber attack on the Ukrainian power grid* (ICS Defense Use Case n.º 5). SANS Industrial Control Systems e Electricity Information Sharing and Analysis Center. https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt6a77276749b76a40/607f235992f0063e5c070fff/E-ISAC_SANS_Ukraine_DUC_5%5B73%5D.pdf

Lexology. (2024, 14 de novembro). *Se aprueba la Ley para la protección de datos personales y la Ley de ciberseguridad y seguridad de la información*. https://www.lexology.com/library/detail.aspx?g=2d00bc2b-a646-4f23-bd68-956d2d5b1afa

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones. (2023). *Estrategia nacional de ciberseguridad de Costa Rica 2023-2027*. https://www.micitt.go.cr/sites/default/files/2023-11/NCS%20Costa%20Rica%20-2010Nov2023%20SPA.pdf

Ministerio de Tecnologías de la Información y Comunicación. (s.d.). *Poder Ejecutivo oficializa la Estrategia nacional de ciberseguridad 2025-2028*. https://mitic.gov.py/enc2025-2028/

Ministerio de Tecnologías de la Información y Comunicación. (2025). *Estrategia nacional de ciberseguridad de Paraguay 2025-2028*. https://mitic.gov.py/eoj0cad9uplo/2025/05/ENC-Paraguay-2025-2028-Mayo-2025 1558.pdf

Osinergmin. (2014). *Resolución n.º 270-2014-OS/CD: estándares técnicos mínimos*. http://www.coes.org.pe/portal/browser/download?url=Marco+Normativo/Base+Legal/05_NORMATIVA+EMITIDA+POR+EL+OSINERGMIN/Res.+N%C2%B0+270-2014-OS-CD.pdf

Paraguai. (2020). *Ley n.º 6534/2020: Ley de protección de datos personales crediticios*. https://www.bacn.gov.py/leyes-paraguayas/9417/ley-n-6534-de-proteccion-de-datos-personales-crediticios

Peru. (2011). *Ley n.º 29733: Ley de protección de datos personales*. https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/243470-29733

Peru. (2020). *Decreto de Urgencia n.º 007-2020: marco de confianza digital*. https://www.gob.pe/institucion/pcm/normas-legales/395322-007-2020

Peru. (2024, 14 de fevereiro). *Decreto Supremo n.º 017-2024-PCM: reglamento de la Ley de Ciberdefensa*. El Peruano. https://www.congreso.gob.pe/Docs/DGP/DIDP/files/ds_017-2024-pcm.pdf

Peru. (2025, 4 de novembro). *Decreto Supremo n.º 126-2025-PCM: reglamento del Decreto de Urgencia n.º 007-2020*. El Peruano. https://busquedas.elperuano.pe/dispositivo/NL/2455024-1

Secretaría de Gobierno de Modernización. (2019). *Resolución 829/2019: Estrategia nacional de ciberseguridad*. Boletín Oficial. https://www.boletinoficial.gob.ar/detalleAviso/primera/208317/20190528

Secretaría de Gobierno de Modernización. (2019). *Resolución 1523/2019: definición de infraestructuras críticas*. Boletín Oficial. https://www.boletinoficial.gob.ar/detalleAviso/primera/216860/20190918

SektorCERT. (2023). *The attack against Danish critical infrastructure* [Relatório técnico]. https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf


adelat