adelat

www.adelat.com

GRIDS UNDER ATTACK

POWER SECTOR CYBERSECURITY IN THE ERA OF ENERGY TRANSITION



DSO Review No. 11 · Series: Technology and Operations

AUTHORS

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

CONTRIBUTORS

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.

KEYWORDS

Cybersecurity; electricity distribution; Latin America; energy transition; critical infrastructure; operational technology (OT); cybersecurity maturity; cybersecurity regulation; tariff recognition; cyber resilience

© 2026 Asociación de Distribuidores de Electricidad de América Latina (ADELAT). All rights reserved. Reproduction in whole or in part for non-commercial purposes is permitted, provided the source is cited.

August 2026

1. INTRODUCTION 4

2. CYBER RISK IN DISTRIBUTION SYSTEMS 6

3. CYBERSECURITY DIMENSIONS AND THE CURRENT STATE OF THE SECTOR 9

3.1. Security of the operational infrastructure 9
3.2. Detection and response capability 11
3.3. Third parties, cloud services, and data protection 12
3.4. Organizational culture and specialized talent 13
3.5. Governance, budget, and the role of the board 15

4. THE REGULATORY RESPONSE IN LATIN AMERICA 17

4.1. The context 17

5. INTERNATIONAL REGULATORY APPROACHES AND BEST PRACTICES 23

5.1. United States: mandatory federal rules for the bulk power system, voluntary state approaches for distribution 24
5.2. European Union: from horizontal legislation to a sector-specific network code 25
5.3. United Kingdom: the energy regulator as cybersecurity authority 28
5.4. Australia: proportionality as a design principle 29
5.5. Ontario: maturity-based regulation for a diverse set of distributors 30
5.6. India: regulating a large-scale system with uneven maturity 31
5.7. Mechanisms that international experience puts on the table 31
5.8. Takeaways for Latin America 34

6. CONCLUSIONS AND REGULATORY RECOMMENDATIONS 36

7. REFERENCES 39

01

INTRODUCTION

The energy transition has become one of the most widely supported transformations of our time: demanded by citizens, embraced by governments, and already underway around the world, driven by technology. Its purpose is to decarbonize the economy by making clean electricity the main energy carrier, and it takes shape in grids equipped with smart metering, remote control, and automated operation, in distributed generation, and in the growing electrification of transport and end uses. Latin America is no exception: its energy plans and regulatory agendas already commit a large share of that modernization, in a context where the need to digitalize the grid is becoming ever more pressing.

This digitalization, while necessary and enabling, has a less visible consequence. As the grid gains intelligence and connectivity, it also gains exposure, since any digital device can be accessed remotely by unauthorized third parties, whether to extract its data, alter its behavior, or take it out of service. Every new smart meter, connected inverter, or remotely controlled device that goes into operation is, at the same time, a new entry point into the infrastructure on which supply depends. The grid's attack surface thus grows at the same pace as the transition itself.

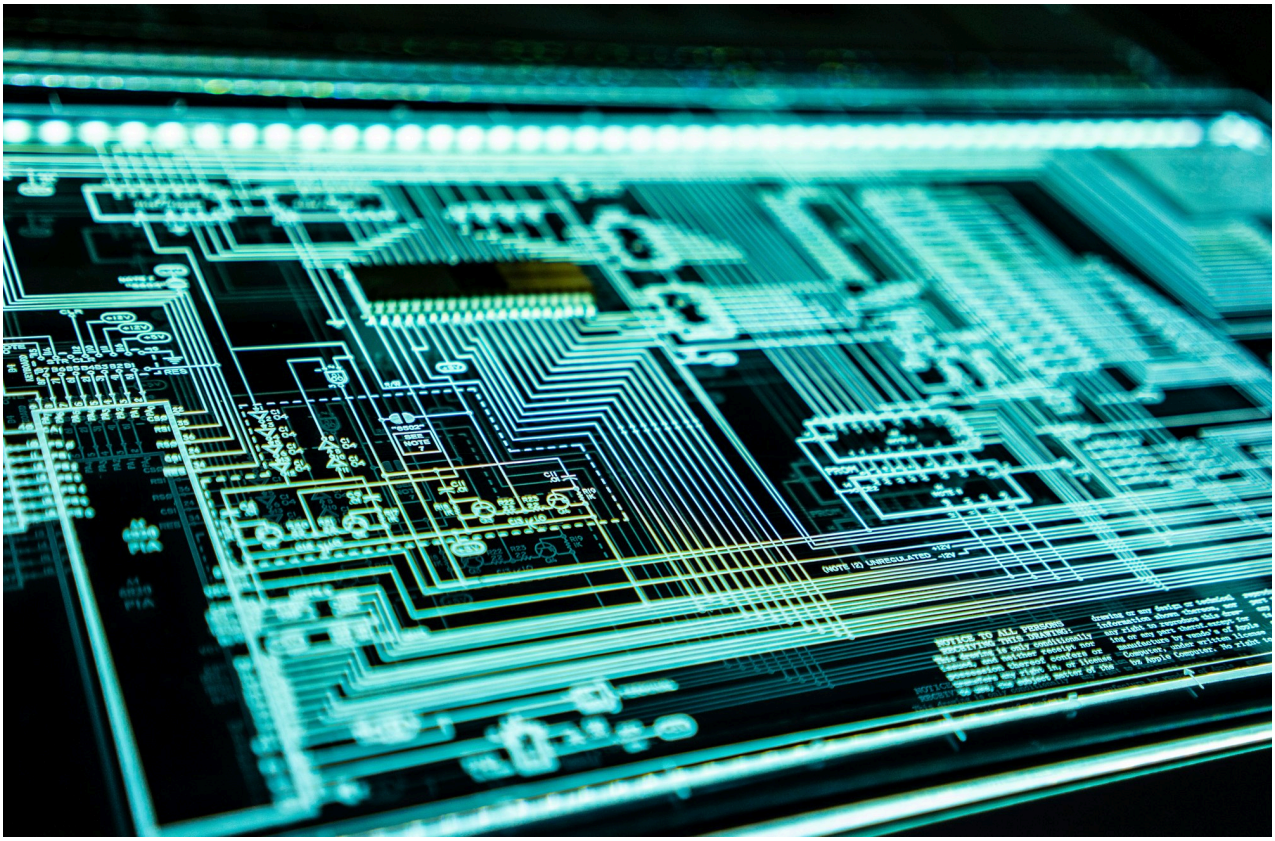
The seriousness of this exposure does not lie in the IT breach itself, but in the fact that its consequences pass directly into the lives of users. For someone left without electricity, it makes no difference whether the outage was caused by a storm or by a cyber intrusion, because the effect is the same: businesses at a standstill, homes in the dark, and essential services running on backup power. Regulation does not distinguish between one cause and the other either, since the outage is recorded in the same continuity indicators that are required and penalized. What changes is the cause and what it takes to prevent it, because an attack does not depend on the weather, it can be repeated, and it can choose the moment of greatest damage, and none of the measures that regulation recognizes and remunerates today, from preventive tree trimming to network reinforcement, can prevent it. On top of the supply interruption come other harms that the traditional grid could not cause, such as the leak of consumption data from millions of customers, which reveals routines and whether people are at home and cannot be undone by restoring service, or the physical damage to equipment by whoever manages to control it remotely. A successful cyberattack against a distribution utility is therefore experienced not as an IT incident, but as an attack on the critical infrastructure on which the daily life of an entire region depends.

The diagnosis that follows rests on primary evidence gathered from the distribution utilities themselves. As part of its Benchmarking Program, ADELAT carried out an exercise devoted to cybersecurity maturity, with the participation of distribution utilities from across Latin America and of very different sizes, from rural cooperatives to large groups with millions of customers. Its results describe a sector in motion, in which some companies have reached high levels of maturity while a significant share is still building basic capabilities. The most relevant finding, however, is not the average level but its internal distribution: the greatest progress is seen in the separation between corporate and operational networks, an area where the sector has historically concentrated its investment, and the deepest gaps are in field devices, which are precisely the ones the energy transition multiplies. Exposure,

then, is growing fastest where the capacity to contain it is weakest.

The source of this disparity lies not mainly in the companies' willingness, but in the framework that shapes their investment decisions. In most countries in the region, cybersecurity is not defined as a sector obligation with its own verifiable standards, and where general legislation on the subject already exists, its application to the distribution segment has not yet translated into operational requirements or into recognition of its cost. Each distribution utility must therefore fund its protection by diverting resources from line items that are recognized, so the level of security ends up depending on each company's conviction and financial headroom, which explains the dispersion the benchmarking reveals. This lack of definition is compounded by a deeper design problem: protecting a digitalized grid is not an investment made once but a capability that must be sustained over time, while tariff frameworks are built to recognize physical assets rather than ongoing operational capabilities. The result is a mismatch that regulation itself creates, as it drives the digitalization of the grid on one track while neglecting, on the other, the conditions needed to protect it. Closing that mismatch means defining the requirement, scaling it to each company's size and criticality, and recognizing its cost within regulated revenues: three decisions that other jurisdictions have already taken and that remain pending in Latin America.

The document is organized as follows. Chapter 2 characterizes the cyber risk specific to distribution networks and what sets it apart from corporate IT security. Chapter 3 sets out the dimensions that make up maturity in this field and presents what the benchmarking reveals in each of them. Chapter 4 examines the state of regulation in Latin America and the scope of the requirements in force. Chapter 5 reviews the experience of jurisdictions that have already faced this problem and draws out the design criteria applicable to the region. Chapter 6 summarizes the regional picture and makes recommendations for regulators.



02

CYBER RISK IN DISTRIBUTION SYSTEMS

The cybersecurity of a distribution network is not the same as that of an office. Every distribution utility is home to two digital worlds: that of the corporate systems that manage billing and commercial information, and that of the operational systems that monitor and control the physical grid[1]. Protecting the latter is a problem of a different nature, because its assets are spread over thousands of kilometers without permanent surveillance, much of the equipment was designed before connectivity and operates with service lives of twenty years or more that do not allow updates, and everything happens in real time, so that stopping a system to inspect it is already the damage one seeks to avoid. Priorities are also reversed: in the corporate domain, the confidentiality of information comes first, whereas in operations what must be protected is the availability and integrity of control, which is why standard IT security practices fall short. That distance between the corporate perimeter and operations is also what determines the severity of an incident, because what matters is not whether an attack occurs but how far it manages to reach.



The attacks already documented against power companies can be ordered by that criterion, and at the first of these levels the attack does not reach the grid. Ransomware[2] gets in through corporate systems and takes billing, the online customer portal, and customer service out of action for days while supply continues unaffected; at this same level are leaks of commercial information, one of which, in the region, put more than fourteen million customer records with addresses and meter numbers into circulation, according to press reports that the affected company

[1] The industry refers to corporate information systems as IT environments and to the systems that monitor and control physical processes as OT (operational technology) environments.

[2] Malicious software that encrypts an organization's data and keeps it unusable until a ransom is paid in exchange for the decryption key.

never confirmed (Adaptix Networks, 2022). All of this tends to be read as an administrative crisis, but it does not always stay there, because when a company cannot determine how far the intruder got, it resorts to a preventive shutdown of operations, as happened in Denmark in 2023, where twenty-two energy companies were compromised through a vulnerability in a supplier's equipment and several chose to disconnect from data networks (SektorCERT, 2023). This is far from exceptional: three out of every four ransomware incidents handled in industrial environments end up degrading operations, and one in four brings them to a complete halt (Dragos, 2025). Stopping service, then, does not require reaching the control systems.

The next level reaches the control systems, and there the incident stops being the company's problem and becomes a supply outage. In December 2015, attackers took control of three Ukrainian distribution companies and opened breakers remotely, just as an operator would have done, leaving 225,000 customers without electricity, while a parallel attack flooded the call center to keep those same customers from reporting the outage. Restoration required sending crews to operate the substations by hand, because remote control had stopped responding, and several communication devices were rendered useless after their firmware[3] was wiped (Lee et al., 2016). A year later, the industrial malware[4] known as Industroyer did away with the human operator and spoke directly to substation protocols on its own, cutting power to part of Kyiv for about an hour (Cherepanov, 2017). In 2022, an updated version of the same program was detected and neutralized hours before it was due to run (CERT-UA, 2022; ESET Research, 2022). The capability exists, has been proven in the field, and continues to be refined.

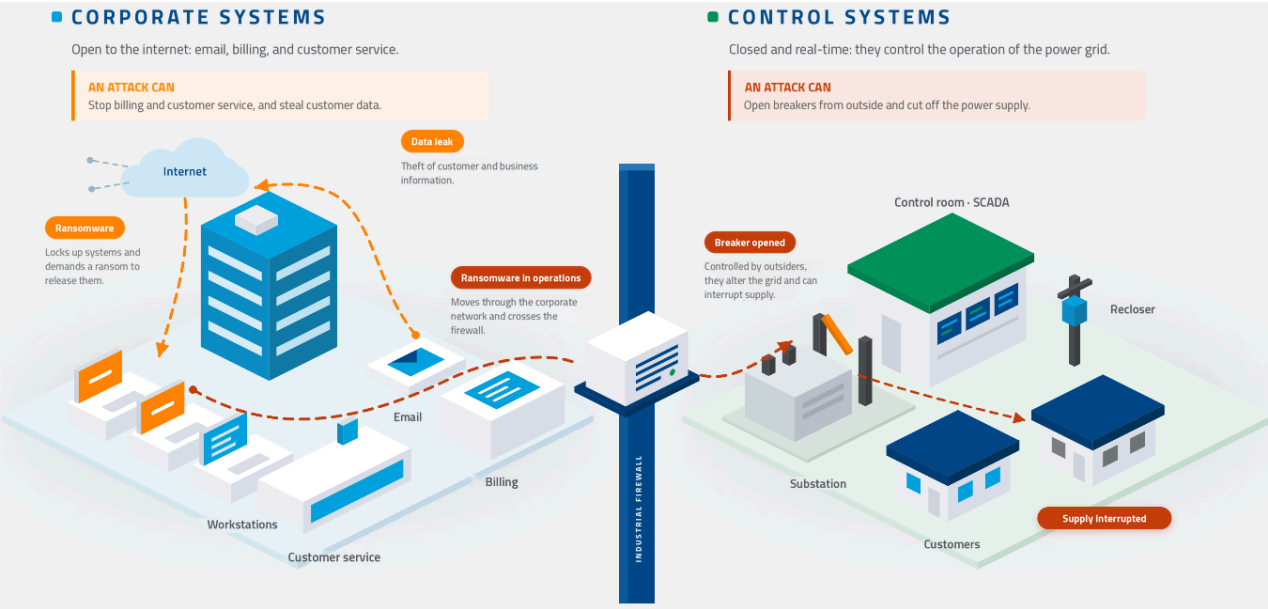


Fig. 1. The two levels of a cyberattack against a distribution utility

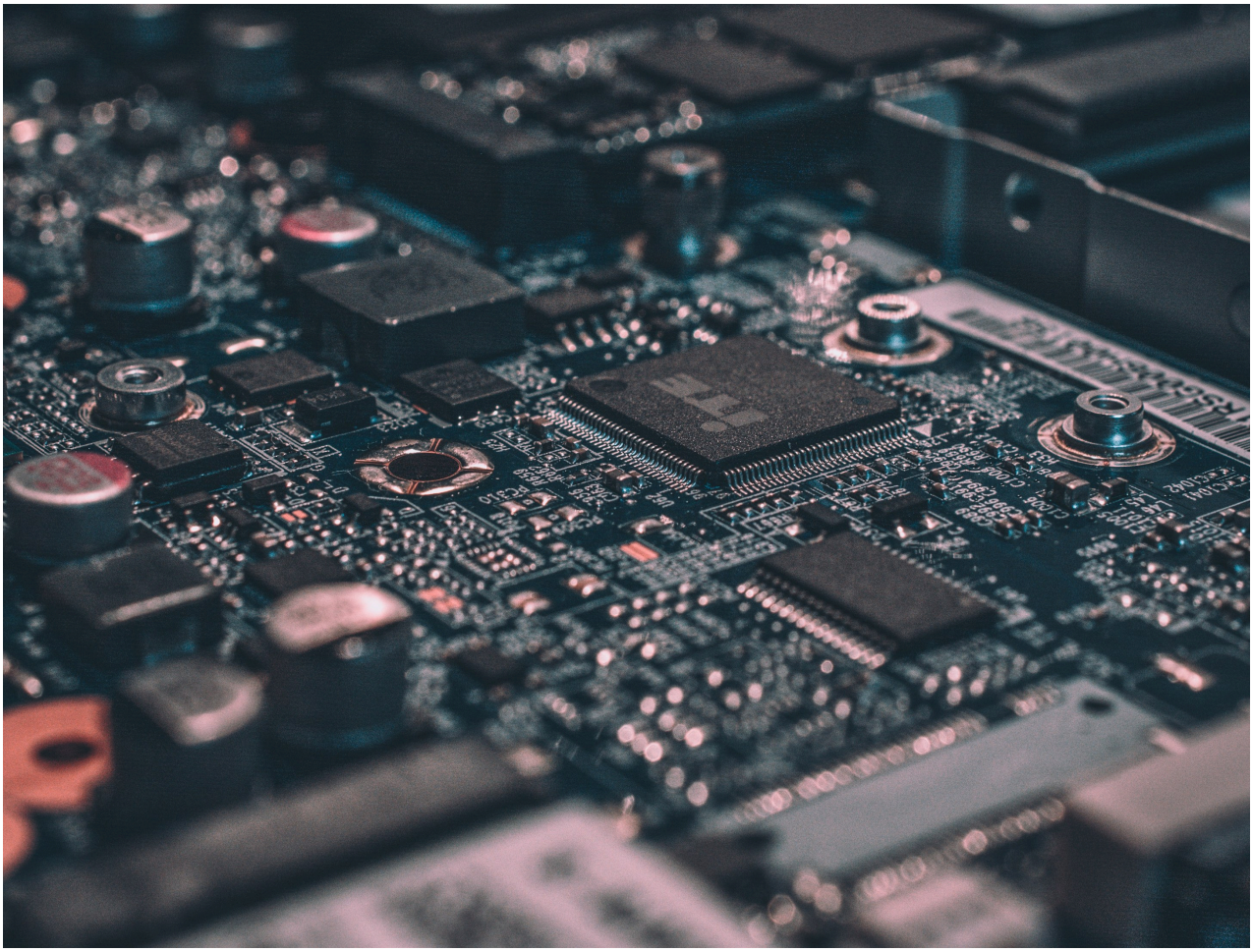
The fact that the regional record is concentrated at the first level does not justify concluding that the second is out of reach, because until recently Latin America had

[3] Software stored in the device's own memory that governs its basic operation. Unlike an application, it cannot easily be uninstalled or reinstalled remotely: recovering it usually requires physical intervention on the device.

[4] Term for any software designed to damage a system, alter its operation, or gain unauthorized access to it. Ransomware is one of its variants.

no obligation to report incidents, and where that obligation did appear, it came after an attack had occurred in that same country, so the available map describes the state of regulation better than the state of the threat. Nor, for the incidents that have occurred in the region, is there any independent investigation establishing whether operations remained intact by design or because the attacker was not prepared to cross over. Rigor also calls for the opposite caveat, since episodes attributed by the press to cyberattacks turned out to be operational failures, such as the blackout that hit Argentina and Uruguay in 2019 (La Tercera, 2019). What can be measured is each company's capacity to contain an attack before it reaches operations, and that is the subject of Chapter 3.

> The capability exists, has been proven in the field, and continues to be refined.



03

CYBERSECURITY DIMENSIONS AND THE CURRENT STATE OF THE SECTOR

A distribution utility's security is not resolved on a single plane, nor does it degrade uniformly, so a diagnosis that is useful to the regulator first requires a common vocabulary. This chapter builds one around five dimensions that structure the problem, from the protection of the infrastructure that operates the grid to the governance that decides on and funds that protection, and between them the capacity to detect and respond, the exposure introduced by third parties and the handling of user data, and the people who sustain all of the above. Each dimension is first explained in its own terms and then illustrated with the self-reports that twenty-five distribution utilities from ten Latin American countries submitted to ADELAT's Benchmarking Program, which therefore reflect the position each company attributes to itself rather than an external verification of its controls. Since the purpose of this diagnosis is to establish where the sector has made progress, where it has not, and how much of that depends on decisions the company itself does not control, all information is presented anonymously and in aggregate form.

3.1. SECURITY OF THE OPERATIONAL INFRASTRUCTURE

The distribution grid stopped being an exclusively physical system when operations began to be carried out remotely. Today a substation opens or closes a breaker because it receives an instruction that travels over a data network, and that instruction cannot tell whether it was sent by an operator or by someone who managed to take their place. This is the layer that Chapter 2 identified as the decisive frontier, because before it the company still decides whether to interrupt service, and beyond it the attacker decides. For decades its protection was organized around a ring: the separation between the operational network and the corporate network. The regional diagnosis asked about that ring, about the channels that must cross it so that operations can be carried out remotely, and about the devices installed out in the territory, which belong to the operational network but sit where no perimeter reaches. The three answers describe a slope that drops as protection moves away from the control center, and that follows the same order in which grid modernization pushed operations outward.

The ring separates two networks that the company needs to keep apart. The corporate network, which must be open to the internet and to hundreds of users, carries email, billing, and management systems. The operational network carries the commands that control the breakers. When the two are one and the same, whoever opens an infected file on an office computer is connected to the control system with no barrier in between, and segregation consists of putting that barrier in place. Fourteen of the 23 companies that responded built it with industrial firewalls and an intermediate zone, so that everything crossing over passes through a device capable of reading electrical protocols and distinguishing a legitimate instruction from one that is not, and another three keep the operational network isolated, with data that goes out but never comes in. The remaining six rely on the configuration of shared network equipment or, in two cases, have no defined perimeter at all.

The ring cannot be continuous, because remote operation requires channels that

cross it. A substation without permanent staff needs to be managed from elsewhere, so these channels exist by design rather than through negligence, and remote access is what makes an extended grid operable. The question, then, is not whether they exist but who comes in through them and with what record. The most common mistake is treating the VPN[5] as the solution, because it encrypts what travels but does not verify who is on the other end, and a stolen credential comes in through that same tunnel without raising suspicion. Twelve companies already require a second authentication factor, which secures the entry but not what happens afterward. The end goal is for permission to be created for a specific task, expire when the task ends, and be recorded, so that between one job and the next there is no standing access to steal, and only one of the twenty companies that responded has achieved it.

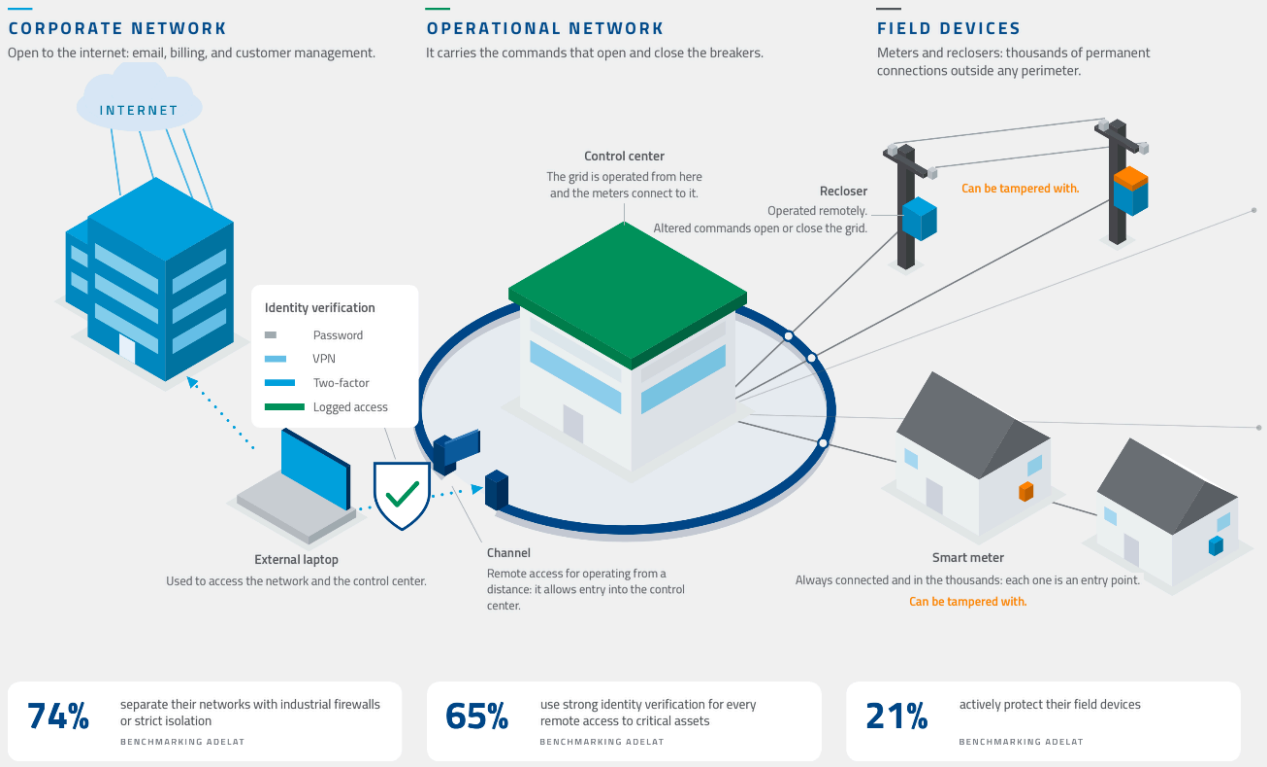


Fig. 2. The three fronts of the operational infrastructure

Field devices are, in practice, permanent channels. A smart meter or a recloser stays in constant communication with central systems to report measurements and receive commands, so each installed device is a connection that is not opened for a task and then closed, but lasts as long as the device remains on the pole. And these are not a few monitored openings but thousands or millions of points on poles and street cabinets, beyond the reach of any perimeter. On the other side, there is no person whose permissions can be revoked, but a device whose identity came from the factory and is usually the same across the whole fleet, so taking one down from a pole is enough to obtain them all. Much of this equipment was installed to last twenty or thirty years and cannot be patched, so companies manage it through containment rather than updates, as the open-ended responses from across the region describe. The end goal is for each device to have its own identity and

[5] VPN: Virtual private network. An encrypted channel that protects information while it travels over a public network but that, on its own, does not verify the identity of whoever uses it.

encrypted communications, and only one of the 19 companies that responded reports having achieved it, while five still use the manufacturer's default credentials.

Ranked by performance, the three fronts are also ranked by the nature of their cost. The ring, which is built once and can be considered finished, is the best-resolved front, with 74% of companies at an advanced level. The channels, whose controls are deployed once but only protect if someone manages every addition, every removal, and every permission every day, fall back to 65%. And field devices, whose cost depends not on how many people must be managed but on how many devices are installed, and which grows with every smart metering program, drop to 21%. The sector's performance declines as the cost stops looking like an investment and starts looking like a permanent operating expense. That correlation points to remuneration schemes, because tariff frameworks recognize investment entering the asset base with relative ease and treat recurring expenditure as a cost to be squeezed in the name of efficiency, so the part of cybersecurity that is most needed is also the part the regulatory model is least able to pay for.

3.2. DETECTION AND RESPONSE CAPABILITY

Monitoring consists of continuously examining the signals the infrastructure generates. A distribution utility's systems, both corporate and operational, produce alerts and logs at all times, and a security operations center (SOC) is the unit that watches them, correlates them, and determines which ones require a response. The utilities' answers range from no monitoring at all to a SOC specialized in the power sector, with analysts able to interpret grid operations as well as corporate systems, a level reached by 4 of the 24 companies that responded. The figure that defines the region is at the other end: the 17% with no active monitoring and the 29% that monitor only the corporate network add up to 46% of the sector that does not watch the operational network, so an intrusion there is noticed only once it is already affecting service. When that happens, what is measured is no longer detection but recovery, how long the company takes to restore supply and its systems, and that time is decided before the incident, by the existence of a response plan that establishes who decides, what is disconnected, and in what order service is restored. The spectrum here separates two things that are often confused, having the plan and having rehearsed it, because a plan that has never been tested is just a document, and its first rehearsal ends up being the real incident. Some 43% of companies validate theirs with annual technical drills, the most encouraging figure in this dimension, and only one reports a plan coordinated with national cybersecurity or defense agencies.

Advanced analytics adds a different capability to monitoring: recognizing anomalous behavior rather than already known threats. The distinction matters because the most serious attacks on power grids do not depend on foreign code but on legitimate commands issued by someone who should not have issued them. Faced with an instruction that is valid in form, the barrier has nothing to object to, and what gives the intruder away is the context: a breaker that opens at an unexplained hour, or a sequence of switching operations that no operator would carry out. An anomaly detection system learns what normal grid operation looks like and raises an alert when something departs from it, and the operational network is especially well suited to this approach because its traffic is repetitive and predictable, far more so than corporate traffic, so anything unusual stands out. The sector is already moving toward this capability: of the 22 companies that responded, 8 have it in place, with production systems monitoring network traffic and email, and another 5 are evaluating it in pilots or proofs of concept, limited trials

designed to test its performance in their own environment before extending it to operations. At the top end, one company reports predictive models protecting critical infrastructure.

What unites the three capabilities is that none can be treated as a construction project. Monitoring is a shift that never ends, a plan is only as good as its last rehearsal, and detection models are retrained as the grid changes. There is nothing here that can be built once, capitalized, and considered finished, and the market itself confirms this: of the 13 companies with continuous monitoring of both networks, 9 contract it as an outsourced service, that is, a monthly invoice rather than an asset. Performance reflects this difference: continuous monitoring of both networks is achieved by 54% of companies, a rehearsed plan by 48%, and anomaly detection in operations by 41%, while the separation between corporate and operational networks, which is built once and financed as an investment, reaches 74%. Outsourcing has already solved how to provide these capabilities even for mid-sized companies, so the barrier is neither technological nor a matter of supply. What remains unsolved is how to pay for them, because a monitoring subscription is exactly the kind of recurring expense that tariff frameworks squeeze.

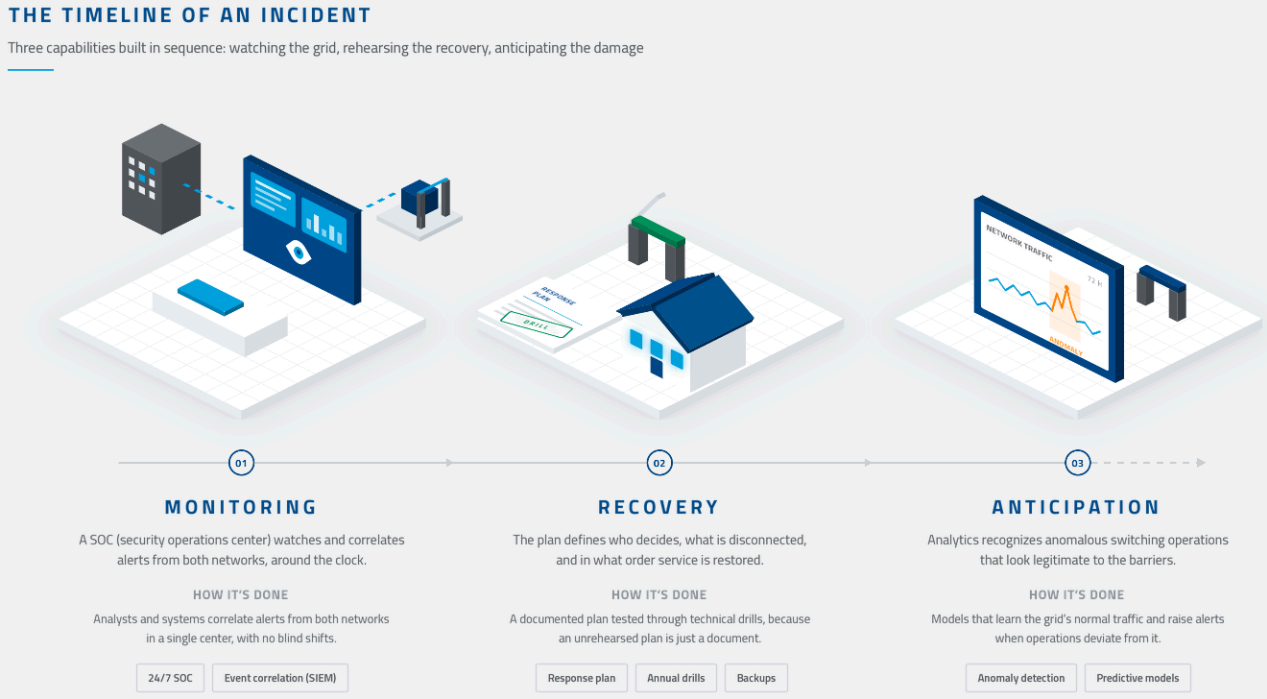


Fig. 3. The capabilities that manage the timeline of an incident

3.3. THIRD PARTIES, CLOUD SERVICES, AND DATA PROTECTION

A growing share of a distribution utility's security and operations is carried out outside the company. Monitoring is contracted as a service, systems are hosted in third-party clouds, equipment arrives with its manufacturer's software, and contractors access the grid to maintain it, so the company's exposure no longer ends at its own infrastructure. That extension stopped being a hypothesis in 2023, when twenty-two Danish energy companies were compromised simultaneously through a vulnerability in equipment from the same supplier. The weak point was not in any of their defenses, but in a device they had all bought. The diagnosis asked about the three sides of this front: supply chain security, the protection of customer data, and the safeguarding of the company's own information.

The supply chain matters because the company inherits the security of everything it buys. Every system acquired comes with its manufacturer's software, every contractor connects with their own credentials, and every cloud service in turn relies on providers that the distribution utility neither chose nor knows, an opacity the companies themselves describe as among their greatest concerns in the diagnosis's open-ended responses. Practices range from not assessing risk in procurement at all to subjecting every acquisition to technical vulnerability testing. Half of the companies (12 of 24) are on the contractual rung, with cybersecurity clauses and audit rights in their contracts, and only one reports prior technical validation. The difference between the two rungs is the difference between paper and verification, because a clause assigns responsibilities and enables audits but does not examine the equipment being purchased, and the right to audit only protects if it is exercised.

Data poses the same problem in two directions. Outward, the company holds the consumption records of millions of customers, which reveal routines and whether people are at home, a harm that cannot be undone once it occurs. Inward, it stores information that is valuable to anyone preparing an intrusion, the grid's maps, the location of its equipment, and the configuration of its systems, which in the wrong hands become the map of the attack. On the first front, 57% of companies report aligning with local data protection law and only 26% add encryption and strict access controls to their commercial databases. On the second, half rely on blocking ports and peripherals, a physical control for a problem that is no longer physical, and 6 of 21 maintain active monitoring of how their sensitive information circulates. On both fronts, most companies stop where the legal obligation ends, and measures that go beyond that minimum, encrypting databases and monitoring what information leaves and through which channels, remain the exception.

The three sides of this front rest on instruments that are exercised once: the clause is signed, the declaration is requested, the law is complied with, and once exercised they can be considered done. Verifying, by contrast, is a permanent task, auditing the supplier, encrypting databases, monitoring the information in circulation, and that is where the sector stops: half of the companies secure by contract what only one checks in the field, and most protect their customers' data as far as the law requires while encryption remains the exception. The regulatory reading has two sides. The first repeats that of the rest of the chapter: the effort that gets postponed is always the permanent one. The second is new, because personal data protection is the front where the legal obligation arrived first and in more countries of the region, and it is also the only one where most companies converge on a common standard. Where there was regulation, there was a floor; where there is none, protection is left to each company's discretion.

3.4. ORGANIZATIONAL CULTURE AND SPECIALIZED TALENT

The barriers, monitoring systems, and contracts covered in this chapter share one condition: someone configures and manages all of them. That dependence has two sides. The first spans the entire organization, because any employee with an email account is a point of entry, and the fraudulent message that obtains a password remains one of the most frequent starting points of an attack. The second is narrower and scarcer: defense systems require specialists who understand both IT security and power system operations. The diagnosis asked about both, awareness among staff as a whole and the availability of that specialized talent.

Awareness means preparing all staff, not just technical staff, to recognize deception attempts that arrive through everyday channels: email, messaging, a phone call. Training ranges from none at all to a secu-

rity culture measured with indicators by area, and in between lies the distinction that matters, the difference between informing and training. Occasional talks inform, but the habit of distrust is acquired through practice, which is why today's standard is phishing[6] simulations, fraudulent emails that the company itself sends to its staff to measure who opens them and to reinforce those who fall for them. Some 44% of companies already run annual programs with this type of exercise and an additional 12% report a continuous culture with behavioral indicators, while the remaining 44% are split between occasional talks and no program at all.

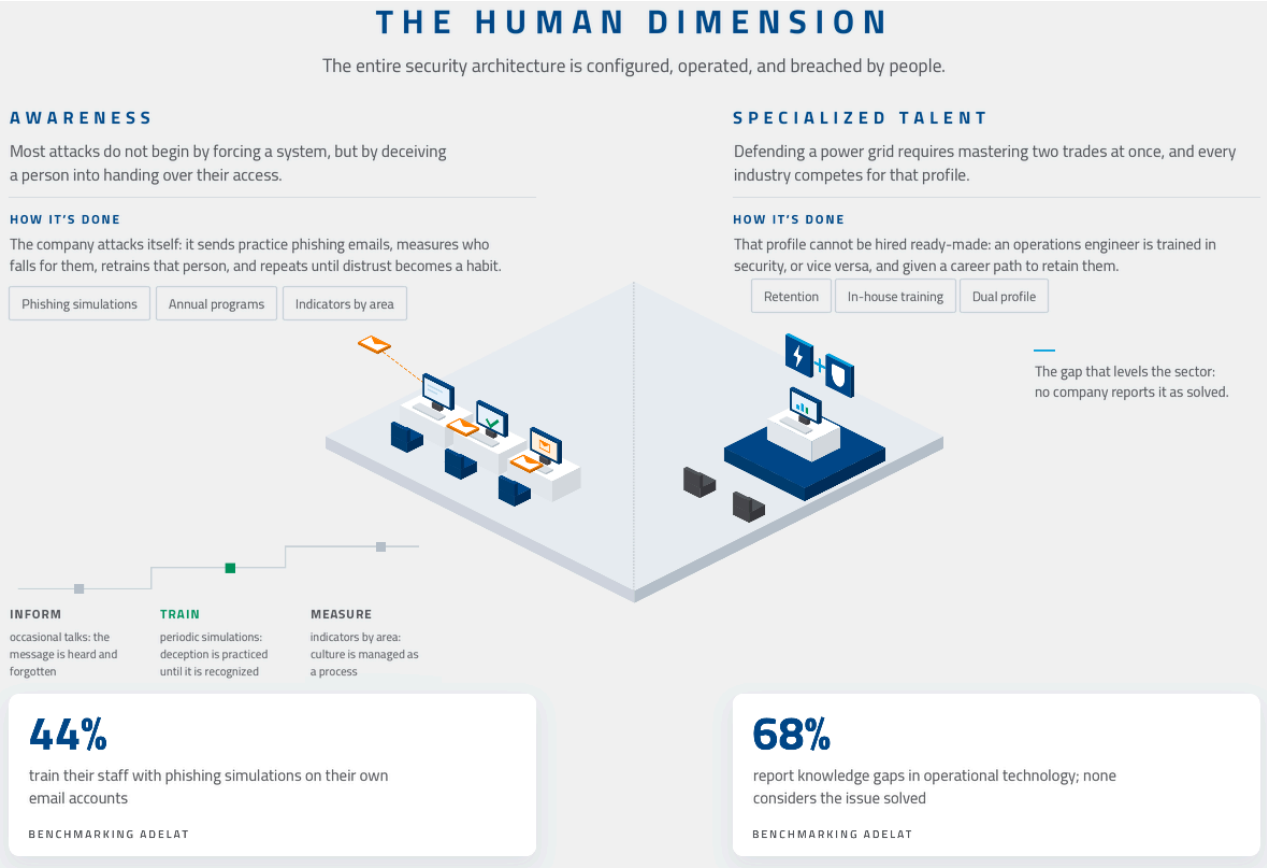


Fig. 4. The human dimension: awareness and talent

Specialized talent is where the diagnosis delivers its most uniform result. Securing a power grid requires a dual profile, someone who understands the protocols and timing of operations and, at the same time, IT attack and defense techniques, a combination that is scarce in labor markets worldwide and that other industries compete for with higher salaries. The responses reflect this without nuance: 17 of the 25 companies, or 68%, report the same situation, a stable team but with knowledge gaps in specific areas, operational technology among the first, and none reports having the profile it needs fully covered. The remaining 8 are further behind, 5 with no specialized staff and 3 with critical difficulties retaining the staff they have. It is the most concentrated response in the entire benchmarking.

Both sides share the same economics. Training only works if it is repeated, because this year's exercise does not protect against next year's scam, and the specialist is paid every month in a market that

[6] Phishing: An email or message that impersonates a legitimate sender to induce the recipient to hand over their credentials or run a malicious file.

competes for them, so both are pure permanent expenditure, with no asset to show in return. The only difference lies in talent, whose scarcity is not a problem of each company but of the market, which is why it is one of the few gaps in this diagnosis that a company's own budget cannot close.

3.5. GOVERNANCE, BUDGET, AND THE ROLE OF THE BOARD

The four previous dimensions have something in common: none can be sustained by a single decision. Renewing controls, maintaining monitoring shifts, auditing suppliers, and retaining specialists require approvals that recur every year, and that continuity exists only when security has its own place in the company's governance. The diagnosis examined that place on three levels: who is accountable for security and to whom, what resources it has, and what method is used to manage it.

The first level is accountability, and the responses fall into four rungs according to how much autonomy security has and to whom it reports. On the lowest, there is no formal assignment, a situation that applies to a single company. On the second, responsibility is delegated to the head of information technology, and almost half the sector is still there, 12 of the 25 companies. On the third, there is already a dedicated position, a security head or manager who still reports within the technology area, with 6 companies. And on the highest, which another 6 reach, there is a CISO, the executive who reports directly to general management or the board. Moving up matters because each rung brings security closer to the decision-makers: whoever reports within technology competes for the technology budget and reaches the board with a filtered message, while the CISO defends their spending without intermediaries. The picture is completed by how often the board takes up the subject: 8 of the 22 companies that responded only hear reports after a serious incident, when there is nothing left to decide except how much it cost, 10 include it twice a year in their corporate risk matrix, and only one maintains quarterly reporting with indicators. In short, the region has created the position but has not yet given it rank: half of the companies treat cybersecurity as just another IT function, and only one in four gives it a seat where decisions are made.

The second level is the budget, and what the diagnosis reveals is not a problem of size but of visibility. In 6 of the 20 companies that responded, cybersecurity spending does not exist as a dedicated budget line but is spread across other accounts, and spending without a line of its own is neither planned nor defended: it is negotiated every year against everything else and is the first to give way when the budget is cut. The evidence that the condition is the budget line and not the amount lies in the others: of the 14 that did set the spending apart, 12 already allocate at least 3% of their technology budget to it. When security manages to exist as a line item, funding follows. Outside the company the problem repeats itself: the tariff does not set that spending apart either. What is not identified separately does not get funded.

The third level is method, and here the sector shows more progress than it is usually credited with. Seven companies operate with current certification or external audits under international standards, and half already measure their performance with operational indicators: how long it takes to detect an intrusion, how long to respond. What is missing lies at the end of the chain, in risk quantification, because translating the probability and impact of an attack into economic terms is a practice reported by only one of the 23 companies that responded. The rest assess their risk with qualitative matrices and scales, useful for setting internal priorities but silent before those who decide with numbers. That pending translation explains much of this dimension, because a board compares investments in money, and a risk that is not

expressed in money competes for budget as an act of faith. And what holds for the board holds for the regulator, which cannot recognize in the tariff a cost that the industry itself does not yet quantify.

The three levels tell the same story at different heights. Security already has a position but rarely rank, already has spending but often without a budget line, and already has a method but does not yet speak the language in which investments are decided. None of this is accidental, because the four previous dimensions showed that the sector's gaps are concentrated where protection requires permanent expenditure, and permanent expenditure survives only if someone with authority approves it every year, with a budget line from which to defend it and a risk figure to justify it. That is why a distribution utility's technical maturity never stays far ahead of the governance that funds it for long. But internal governance has a limit that this chapter makes clear: it can decide to spend, but it cannot decide that the spending will be recognized in the tariff. That decision belongs to the regulator, and it is the subject of the chapters that follow.

> When security manages to exist as a line item, funding follows.



04

THE REGULATORY RESPONSE IN LATIN AMERICA

Against a backdrop of uneven maturity, in which companies' technical progress still lacks the governance and funding to sustain it over time, the region's regulatory frameworks have begun to move, albeit at different speeds and with different approaches across countries. This chapter examines how the Latin American regulatory environment is responding to cybersecurity risks in the electricity sector.

Chapter 3 documented maturity that is uneven and, above all, incomplete: companies are making progress on technical controls, but that capacity is not underpinned by formal governance, a dedicated budget, or economic recognition. The question now is what regulation is doing about that gap. This chapter sets aside the diagnosis of the companies, already covered, and examines the diagnosis of the rules: what regulatory instruments exist in the region today, whom they bind, what they require, and above all whether they recognize the cost of complying with them. The first section maps the regional regulatory landscape as a whole and sets out the tensions that arise when regulation moves at a different pace from the operational capacity of the companies it must regulate. The second section breaks that landscape down country by country, highlighting how cases such as Brazil and Chile, pioneers in establishing binding sector obligations, coexist with very different operational realities, and how other countries in the sample are still moving forward on the basis of general frameworks that do not always reach private or cooperative electricity distribution.

4.1. THE CONTEXT

Of the countries analyzed, three currently have a binding and enforceable sector-specific electricity cybersecurity obligation for distribution: Brazil and Chile through law and state regulation, and Colombia through a mandatory agreement of the system operator, without the need for a general cybersecurity law. The rest of the sample relies on general cybersecurity frameworks, on schemes limited to the public sector, or lacks dedicated regulation altogether. That asymmetry, three countries with a firm sector obligation and eight without one, is the first fact that any regulatory proposal must take as its starting point, and it is detailed country by country in the following section.

The region shares, without exception, the same gap: none of the regulatory frameworks recognizes cybersecurity as an explicit, stand-alone tariff line item. Where the obligation exists, the cost of complying with it is diluted across generic operating, maintenance, or investment items. This is the most relevant regulatory tension for an association of distribution utilities, because it means that regulation can require a control without yet opening the way to fund it.

A second tension arises between the technical requirement and its regulatory recognition. Chile is the country that has gone furthest in building the regulatory apparatus, with a framework law, an enforcement agency, a national CSIRT[7], and its own electricity technical standard, all in less than two years (2024-2026), but that same framework does not yet provide for tariff recognition of the investments it requires.

[7] CSIRT: Computer Security Incident Response Team, a specialized team that receives incident reports, coordinates the response, and disseminates alerts among the organizations it serves.

Technical compliance, in other words, can become mandatory before the economic regulation needed to sustain it exists.

A third tension concerns sequencing: sector regulation can arrive before the operational capacity of those it binds. Brazil was the first country in the region to issue a binding sector-specific electricity regulation (ANEEL 964/2021, in force since 2022), but it applies it uniformly to distribution utilities of very different sizes and capabilities, without adjusting the pace of the requirements to the size of the regulated company. It is the opposite regulatory risk to Chile's: while there the institutional architecture runs ahead of funding, in Brazil the obligation runs ahead of the smaller companies' capacity to comply with it.

These three tensions, the universal tariff gap, technical requirements without funding, and regulation without differentiation by capacity, are not evenly distributed across the eleven countries. Latin America is not moving at the same pace on electricity cybersecurity, but neither is it moving in unrelated directions. A look at the eleven countries analyzed reveals three groups with distinct profiles: a mature core made up of Brazil, Chile, and Colombia, where sector regulation already binds distribution utilities; an intermediate group, Peru, Argentina, and Ecuador, which in just two years built national institutions that have not yet fully reached the electricity sector; and an early-stage group, Costa Rica, El Salvador, Guatemala, Bolivia, and Paraguay, which is only beginning to discuss who should govern the issue.

The most revealing point, however, is not the distance between these groups but what they all have in common. No country in the region, not even the most advanced, recognizes cybersecurity as an explicit, stand-alone tariff line item. Costs, where they exist, are diluted across generic operating, maintenance, or investment plan items. It is by far the most relevant finding: the legal framework is advancing, but the economic framework that should sustain it does not yet exist anywhere.

The comparative table yields five findings worth establishing before the country-by-country review:

- Complete absence of a cybersecurity tariff line item. In none of the eleven countries does cybersecurity appear as an explicitly recognized, stand-alone tariff component.
- A sector-specific electricity obligation is clear and mature only in Brazil, Chile, and Colombia, where the regulation expressly mentions distribution utilities and sets deadlines or a penalty regime.
- A truly active penalty regime exists only in Chile, with fines for operators of vital importance of up to 40,000 UTM (Chilean monthly tax units) since March 2025.
- The obligation to report incidents now also extends to Peru and Ecuador, although in both cases without a fully enforceable penalty regime yet.
- Almost every country has a national CSIRT (Computer Security Incident Response Team), but only Colombia has a formal electricity-sector CSIRT; in Chile, the role is performed de facto by the specialized unit of the CEN (National Electricity Coordinator).

4.2. DEVELOPMENTS BY COUNTRY

Country	Sector-specific electricity cybersecurity regulation?	Covers distribution?	Incident reporting obligation?	National or sector CSIRT?	Investments recognized in tariffs?
Brazil	Yes – ANEEL Normative Resolution (REN) 964/2021, with active enforcement since Feb/2025 (Despacho 427: periodic submission of monitoring data)	Yes – concessionaires, permit holders, authorized entities, and other agents (G, T, D, system operation, and retail)	Yes – notification to the sector coordination team as soon as the incident becomes known, with analysis of cause, impact, and mitigation	National CSIRT (CTIR Gov); no formal dedicated electricity-sector CSIRT	Not identified – no explicit, stand-alone tariff line item
Chile	Yes – Law 21,663/2024 + CEN Cybersecurity Standard (based on NERC CIP, 2022); NTSyCS (Technical Standard for Security and Quality of Service) of the CNE	Yes – G, T, and D classified as essential services; covers the entire chain, including the CEN itself	Yes – Art. 9 of Law 21,663: early warning within 3 h, initial report within 72 h, final report within 15 days (Decree 295)	Yes – National CSIRT + Defense CSIRT; in the electricity sector, the CEN's Cybersecurity Unit acts de facto as the sector team.	No – no explicit, stand-alone tariff recognition; costs absorbed under general operating and investment regulation
Colombia	Yes – CNO Cybersecurity Guide, Agreement 1960/2025, with a risk-based approach and phased deadlines through 2028	Yes – mandatory for G, T, D, and the operator of the SIN (National Interconnected System)	Yes – CNO Agreement 2088 (Nov/2025)	Yes – colCERT (national CSIRT; Decree 338/2022) + electricity-sector CSIRT	No – CREG Resolution 101-001/2022 treats smart metering cybersecurity as a technical obligation
Argentina	No – no ENRE regulation; Administrative Decision 641/2021 and Provision 1/2026 of the new National Cybersecurity Center apply only to the National Public Sector	Not directly applicable (private distribution utilities not bound)	No – no fixed legal deadline or penalty regime for private distribution utilities	Partial – CERT.ar (national CSIRT)	No – no tariff recognition in the ENRE methodology
Peru	No – no dedicated regulation, only related technical standards that reference NERC CIP (SCADA and availability)	Partial – the related standards cover SCADA and availability, without constituting cybersecurity regulation as such	Yes – Supreme Decree 126-2025-PCM (regulations implementing Emergency Decree 007-2020), in force since Feb/2026, sets 48 h to notify the CNSD; penalty regime still pending	Yes – PECERT (national CSIRT, operated by the National Digital Security Center); no formal electricity-sector CSIRT	Partial and case-by-case – no structured tariff recognition
Ecuador	Yes, since 2026 – Organic Law for the Strengthening of Cybersecurity	Partial – energy recognized as an essential sector, with actual classification expected between Nov/2026 and May/2027	Yes – 72 h notification obligation already in force, with no designated sector oversight body; full penalty regime enforceable within 24 months	Yes – National CSIRT with operational autonomy, not yet formally linked to the electricity sector	No – methodology structured around physical assets, with no equivalent category for digital protection
Costa Rica	No – no sector-specific electricity regulation	Not applicable	No – Directive 133-MP-MICITT requires reporting to CSIRT-CR only within the central public administration	Yes – CSIRT-CR (national, operational)	Not identified

Country	Sector-specific electricity cybersecurity regulation?	Covers distribution?	Incident reporting obligation?	National or sector CSIRT?	Investments recognized in tariffs?
El Salvador	Partial – Decree 143/2024 covers critical infrastructure (including energy); no specific regulation of its own	Yes, in principle (pending technical guidelines)	Depends on future regulations by the ACE	Yes – State Cybersecurity Agency (national); no electricity-sector CSIRT identified	Not identified
Guatemala	No – no general law in force; Initiative 6347 under consideration, subject to public debate and not yet approved	Not applicable	No – no legal reporting obligation in force	No – no consolidated national CSIRT; no electricity-sector CSIRT	There is no explicit tariff recognition mechanism for cybersecurity investments and recurring expenditure.
Bolivia	No – no general law or approved national strategy.	Not applicable	No – no defined deadline or penalty regime	Partial – CSIRT-BO (national CSIRT); no electricity-sector CSIRT	Not identified
Paraguay	No — no dedicated sector-specific electricity regulation	Not applicable	Not identified	Yes — CERT-PY (national); no electricity-sector CSIRT	Not identified

Table 4.1. Electricity cybersecurity regulatory framework by country.

The mature core: Brazil, Chile, and Colombia. These three countries reached regulatory maturity by different paths, and therein lies part of their interest. Brazil did so in the most direct way: the electricity regulator, ANEEL (Agência Nacional de Energia Elétrica), issued its own normative resolution (964/2021) and today actively enforces compliance, requiring periodic submission of maturity and risk data since 2025. Chile combined a national framework law, Law 21,663, in force since March 2025, with a real penalty regime and fines of up to 40,000 UTM, with its own technical standard that the National Electricity Coordinator (CEN) has been applying since 2020, inspired by the North American NERC CIP (North American Electric Reliability Corporation – Critical Infrastructure Protection) standards. Colombia, by contrast, achieved comparable sector development without a general cybersecurity law: the National Operation Council (CNO), drawing on its own rulemaking authority, built a mandatory guide for the entire electricity chain and, in November 2025, its own sector CSIRT.

That last observation, a country without a national framework that nevertheless leads in sector maturity, is perhaps the most interesting parallel within the group: it shows that self-regulation by a system operator with rulemaking authority can move faster than a general law, and that both paths sooner or later converge on similar results: coverage of the entire chain, defined reporting deadlines, and a CSIRT dedicated to the sector.

Even so, none of the three has resolved the tariff knot. Brazil leaves open the possibility that ANEEL may consider cost recognition in the future; Chile and Colombia, for now, do not contemplate it at all.

The intermediate group and the 2025-2026 window. Peru, Argentina, and Ecuador reorganized their cybersecurity institutions at almost the same time, in the final stretch of 2025 and the beginning of 2026. Argentina created its National Cybersecurity Center by a decree of necessity and urgency on December 31, 2025, in force since January 2026. Peru, after five

years of partial application, finally issued implementing regulations for its Emergency Decree 007-2020, published in November 2025 and in force since February 2026, setting a 48-hour deadline for reporting incidents. In the same period, Ecuador approved its first comprehensive organic law on cybersecurity. Even Bolivia, which is at an earlier stage of institutional development, moved its institutions during that same period: Supreme Decree 5519, of January 2026, transferred digital certification responsibilities from ADSIB to AGETIC.

That timing, four countries reforming their institutional architecture within a window of just three months, suggests more than coincidence: it probably responds to a common regional pressure, whether regulatory, geopolitical, or stemming from recent incidents, that pushed several governments to act almost in unison.

What has not yet happened, in any of the three intermediate countries, is for those national institutions to reach the electricity sector. In Peru, the regulator Osinergmin and the system operator COES still lack cybersecurity regulation as such, relying only on technical references to NERC CIP, the same standard that inspired Chile's CEN. In Argentina, the regulations in force apply only to the National Public Sector and do not bind private distribution utilities unless they adhere voluntarily. In Ecuador, the law already recognizes electricity as an essential service, but the actual classification of which assets and companies will be subject to the regime will only take place between November 2026 and May 2027.

The early-stage group: between strategy and regulation yet to be built. Costa Rica, El Salvador, Guatemala, Bolivia, and Paraguay share a common trait: none yet has dedicated sector-specific electricity regulation. But even here there are parallels worth noting. Costa Rica and El Salvador are following the same path: a bill that would create a national cybersecurity agency. In Costa Rica, Legislative File 23,292 has been under consideration since August 2022 and explicitly provides for the future agency to coordinate with sector regulators such as ARESEP. El Salvador has already crossed that line, as its Decree 143/2024 created the State Cybersecurity Agency, but application to the electricity sector is still awaiting technical guidelines that the agency itself has not yet issued. It is, in a way, the same story told at two different moments.

Another parallel links Chile, El Salvador, and Ecuador, countries otherwise far apart in maturity: all three approved their cybersecurity law almost simultaneously with a personal data protection law, Chile with Law 21,719, El Salvador with Decree 144 (the twin of Decree 143), and Ecuador with its Organic Law on Personal Data Protection. This duplication is no accident: the two subjects share triggering events (a data breach is usually also a cyber incident), and in several countries it already creates a concrete risk of duplicate reporting to different authorities, something Ecuador's own law expressly points out.

Paraguay deserves a separate mention because of its structural uniqueness: since it has no independent electricity regulator, as the system is operated by the vertically integrated state-owned company ANDE, it makes no sense even to ask about tariff recognition, because there is no regulated tariff review process to which such recognition could apply. It is the only one of the eleven countries where the tariff gap is not a regulatory omission but a direct consequence of the sector's institutional design.

Within this group, Guatemala and Bolivia are at an earlier stage of institutional development: neither has an approved general law, a fully consolidated national CSIRT, or a classification of critical infrastructure. Guatemala also has a particularity of its own: its bill (Initiative 6347) is the subject of public debate, with no consensus yet on which body should govern the issue.

Beyond the maturity groups, the region's body of regulation reveals some patterns that recur from one country to another.

1. **The 2025-2026 window.** Colombia (CNO Agreement 2088, Nov/2025), Peru (regulations implementing Emergency Decree 007-2020, Nov/2025, in force Feb/2026), Argentina (creation of the National Cybersecurity Center, Dec/2025, in force Jan/2026), and Bolivia (transfer of functions to AGETIC, Jan/2026) reformed their institutions within just three months. It is the clearest sign that the issue gained political urgency simultaneously in governments that, in almost everything else, move at different speeds.

2. **A borrowed standard as a technical anchor**. The North American NERC CIP standards appear as a technical reference both in Chile's CEN standard (2020) and in the related technical standards of Peru's electricity sector. No other international standard recurs as often in the texts analyzed, which suggests a path of de facto technical convergence, even where there is no legal convergence.

3. **Twin laws: cybersecurity and personal data**. Chile, El Salvador, and Ecuador approved their cybersecurity law together with a personal data protection law, almost as a single package. That regulatory proximity multiplies notification obligations for a single incident and foreshadows an institutional coordination problem that no country has yet fully resolved.

4. **National CSIRTs almost universal, electricity CSIRTs almost nonexistent.** Ten of the eleven countries have an operational national CSIRT (CTIR Gov, CSIRT Nacional/Chile, colCERT, CERT.ar, PECERT, CSIRT Ecuador, CSIRT-CR, CSIRT-BO, CERT-PY; El Salvador is the visible exception, with its incident registry under the ACE). But a CSIRT dedicated to the electricity sector exists on a fully formal basis only in Colombia; Chile has one de facto through the CEN. The rest of the region still depends on generic teams for incidents that, by their nature, require specific operational knowledge of substations, SCADA[8], and remote control.

5. **The tariff gap, without exception.** It is the only point on which the eleven countries agree without qualification: in none of them is cybersecurity an explicit, stand-alone tariff line item for remunerated cost or investment. Even where the legal framework is most demanding, in Chile and Colombia, the funding of these obligations still lacks a formal path to recognition.

The regional landscape allows a twofold reading. On the one hand, there is real regulatory movement, in several cases coordinated in time: the 2025-2026 window shows that several governments are taking the issue seriously almost simultaneously, and the three most mature countries already cover distribution utilities with concrete reporting obligations and, at least in Chile, effective penalties. On the other hand, the entire region shares the same blind spot: tariff design has not evolved at the same pace as regulatory design. Until that changes, distribution utilities will continue to invest in cybersecurity with no formal way to recover that cost, a gap that sooner or later will have to be closed in every country, not only in those at an earlier stage.

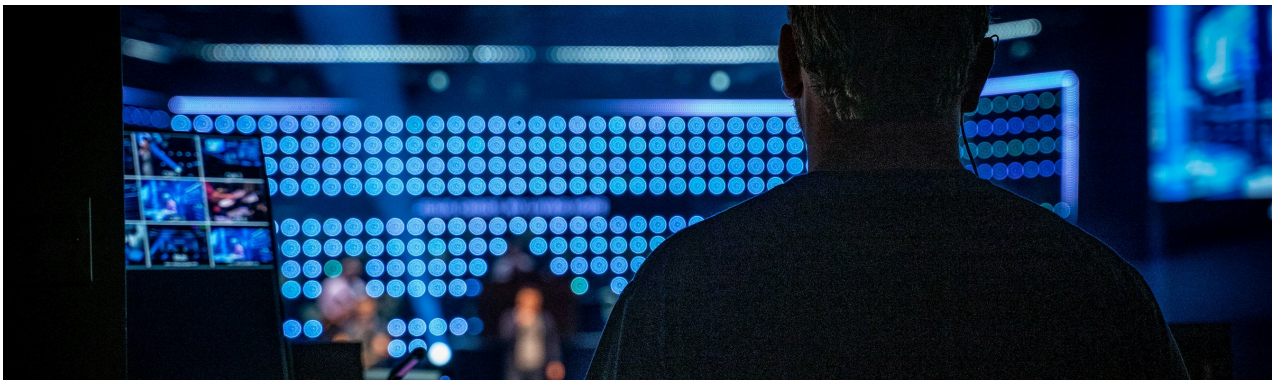
[8] SCADA: Supervisory Control and Data Acquisition, a system that remotely monitors and controls power grid equipment from a control center.

05

INTERNATIONAL REGULATORY APPROACHES AND BEST PRACTICES

The previous chapter finds that electricity cybersecurity regulation is moving in Latin America, but unevenly, with scattered instruments and without resolving who pays to protect a grid that regulation itself requires to be digitalized.

This chapter reviews six jurisdictions that have been regulating the cybersecurity of their power systems for between six and eighteen years: the United States, the European Union, the United Kingdom, Australia, the Canadian province of Ontario, and India. It is important to note that the benchmarks examined rest on institutional assumptions that do not always hold in the region: regulators with their own technical capacity to audit industrial cybersecurity, consolidated national cybersecurity agencies, and tariff frameworks with periodic reviews in which a new line item can actually be included.



To keep the comparison useful and prevent it from becoming a catalog, each jurisdiction is examined through the same four questions: (i) What does it require? Whether the obligation is a verifiable technical control, a management system, or an assessed maturity level; whether it is voluntary or mandatory, and what the consequences of non-compliance are; (ii) Whom does it cover? Whether it covers only the transmission system or distribution as well, and by what criterion the obligated universe is defined: size, criticality, impact, or number of customers; (iii) How is it funded? What instrument recognizes the cost of compliance: a tariff line item, an incentive, a regulatory asset, a business case, or none; (iv) How is it scaled? The proportionality mechanism that allows a rural cooperative and a large group to coexist under the same rule without the former being shut out or the latter underregulated.

Electricity cybersecurity regulation in the developed world was born looking at the transmission system. The United States, the European Union, and Australia built their frameworks around the systemic risk of the bulk power system, and distribution came in later, partially, belatedly, or indirectly. Only three of the six cases reviewed were written explicitly with distribution utilities in mind, and two of them date from the last three years. For Latin America, this has an encouraging reading: the region is not arriving late to a consolidated model, because the regulatory model for distribution is still being written everywhere.

5.1. UNITED STATES: MANDATORY FEDERAL RULES FOR THE BULK POWER SYSTEM, VOLUNTARY STATE APPROACHES FOR DISTRIBUTION

U.S. electricity regulation divides authority by segment rather than by territory. The Federal Energy Regulatory Commission has jurisdiction over interstate transmission and wholesale electricity sales, while distribution and retail supply fall under each state's regulatory commission. That division, which predates any discussion of cybersecurity, determines the scope of the federal regime and explains why the country with the world's strictest requirements for the bulk power system lacks a single mandatory framework for distribution.

The second particularity is institutional. After the 2003 Northeast blackout, federal legislation created the figure of the Electric Reliability Organization: a private entity certified by the federal regulator, with authority to propose standards that, once approved, become mandatory for all users, owners, and operators of the bulk power system. The designated organization, NERC, issues the standards and verifies compliance through regional entities that audit more than a thousand registered entities. It is a co-regulation model: industry drafts the technical standard, the regulator approves it and gives it binding force, and penalties are public.

NERC CIP: mandatory, auditable, and enforceable standards

In 2008, the Commission approved the first family of critical infrastructure protection standards, known as NERC CIP. The set is organized by subject and has grown continuously for almost two decades. It starts with the identification and categorization of the bulk power system's cyber systems and from there sets out requirements on security management controls, personnel and training, electronic security perimeters, physical security of cyber assets, systems and patch management, incident reporting and response planning, recovery plans, change management and vulnerability assessments, information protection, and, since 2020, supply chain risk management.

These are not best practice guidelines but enforceable standards. Compliance is verified through periodic audits conducted by the regional entities, complemented by the obligation to self-report violations and to submit mitigation plans, and backed by civil penalties that can reach the order of USD 1.5 million per day per violation. Penalties are also public: case files and amounts are published, so reputational cost is added to economic cost.

Proportionality is built into the design itself. Each cyber system is categorized into three impact levels, high, medium, and low, according to the consequences its compromise would have on the system, and the set of applicable requirements depends on that categorization rather than on the size of the company that operates it. A large control center and a minor facility are subject to different requirements even if they belong to the same company.

The most recent developments confirm the shift of defense toward the inside of the network. In June 2025, the Commission approved standard CIP-015, which requires monitoring of traffic within electronic security perimeters and not only at their edges, with phased deadlines of thirty-six months for control centers and sixty months for the remaining applicable assets. The stated rationale is that perimeter defenses do not detect an attacker who has already obtained legitimate access, and that recognizing lateral movement[9] in time is the only way to limit the damage.

[9] Lateral movement: An attacker's progression from the system through which they gained entry to other systems in the same organization, exploiting legitimate access and credentials.

Order 893 and the calibration of incentives

The most relevant U.S. precedent on funding arose from a legislative mandate. The 2021 infrastructure law added a section to the Federal Power Act directing the Commission to establish, through a rulemaking, incentive-based rate treatment for investments in advanced cybersecurity. The result was Order 893, of April 2023.

The design recognizes two things. The first is that cybersecurity has a substantial recurring expenditure component and not only an investment component: eligible items include operation and maintenance expenses, labor costs, implementation, network monitoring, training, and certain services contracted on a subscription basis. The second is that effort beyond mandatory compliance deserves differentiated recognition, so the incentive is reserved for voluntary investments that materially improve security posture and are not already required by the CIP standards.

In the end, only one instrument was approved: a cybersecurity regulatory asset that allows those costs to be deferred, included in the rate base, and earn a return on the unamortized portion, with an amortization period of up to five years. The original proposal also included an adder to the allowed return, which the Commission discarded in the final rule. Access was structured around a list of pre-approved items that was reduced to two: participation in the federal threat information sharing program and the deployment of internal network security monitoring.

More than a year after it took effect, no application had been filed. Industry analysts point to a combination of an overly narrow pre-approved list, a procedure requiring a specific rate filing open to challenge by third parties, and a benefit that, for most companies, did not offset that administrative cost. The case is useful precisely for that reason: it shows that tariff recognition of cybersecurity is not achieved by the instrument's existence but by its calibration.

The distribution gap and the NARUC–DOE response

The scope of NERC CIP is the bulk power system. Distribution remains under the authority of state regulators, with markedly heterogeneous results: some states have developed their own requirements or specialized oversight arrangements, others include cybersecurity as a criterion within ordinary rate proceedings, and others have not legislated on the matter.

In the face of this dispersion, the response was not a federal standard but a reference product developed through a public-private process. In February 2024, the national association of state utility regulators (NARUC) and the Department of Energy (DOE) published a set of cybersecurity baselines for distribution systems and the distributed energy resources connected to them, prepared by a steering group made up of state regulators, distribution utilities, operators and aggregators of distributed resources, and security experts.

The product is not a standard. It is a baseline aimed at three different audiences, state commissions, distribution utilities, and operators of distributed resources, and its stated goal is alignment among the states that choose to adopt it, whatever route they take to do so. A second phase, carried out during 2025, produced implementation guides focused on the two problems that experience showed to be critical: defining the universe of assets to be considered and prioritizing among the baseline measures, with differentiated paths depending on whether adoption is voluntary or mandatory and on each company's size, ownership, and maturity.

5.2. EUROPEAN UNION: FROM HORIZONTAL LEGISLATION TO A SECTOR-SPECIFIC NETWORK CODE

European electricity cybersecurity regula-

tion is built on two legal instruments of a different nature. Directives set objectives and must be transposed into each member state's legislation, which introduces variability and time, while regulations apply directly and uniformly. Cybersecurity in the European electricity sector came to be governed by both: a cross-cutting directive covering all critical sectors and a sector regulation that applies directly to electricity.

The second particularity is the instrument chosen for the sector level. Network codes are the mechanism through which the Union harmonizes the technical rules of the internal electricity market, covering connection, operation, balancing, and capacity management, and they are developed through a procedure involving the Commission, the Agency for the Cooperation of Energy Regulators, the European Network of Transmission System Operators, and the EU DSO Entity. The fact that cybersecurity was incorporated through this route means that it is treated as a condition of system operation, on the same footing as frequency or balancing rules, and that its technical development is carried out by the same actors that operate the grid.

NIS2 and the Network Code: two regulatory layers

The 2022 directive on the security of network and information systems, known as NIS2, sets the common floor. It covers entities considered essential, including those in the energy sector, and requires them to manage risk, notify incidents within short deadlines, secure their supply chain, and make their management bodies accountable for overseeing these measures, with penalty regimes that each member state must establish.

Its implementation illustrates a sequencing problem worth noting. Transposition into national law progressed unevenly relative to the planned deadline, and since the sector code relies on definitions, authorities, and procedures created by the directive, that delay also held back its effective application. Without a designated authority, an operational incident response team, and supervisory capacity, the text exists but does not produce security.

On top of that floor sits Delegated Regulation (EU) 2024/1366, in force since June 2024, the first network code of the European electricity sector devoted entirely to cybersecurity. Its obligations are organized around a cybersecurity management system, the sector equivalent of an information security management system, and two sets of controls, minimum and advanced, whose application depends on the entity's impact level. In addition, there are specific requirements on the supply chain, crisis management, periodic exercises, and compliance verification.

The risk management cycle runs every three years and is structured on four levels. A Union-wide assessment identifies the system's critical processes and defines the common impact scale; regional assessments aggregate information from several member states; national assessments are carried out by the competent authorities; and each entity assesses its own perimeter using the common impact matrix. Within twelve months of its designation, and every three years thereafter, each entity must report to its authority the controls selected, the estimated residual risk, and the list of critical technology suppliers involved in critical-impact processes.

Governance is as important as content. The methodologies and controls are not dictated unilaterally by the authority: they are developed by the transmission system operators in cooperation with the EU DSO Entity, with the participation of the energy regulators' agency and the EU cybersecurity agency. Distribution, as a segment, has a formal seat at the table where what will be required of it is defined.

The supply chain controls deserve separate mention because of their logic.

Distribution utilities are not asked to solve the problem of equipment already installed: instead, the conditions for what can be purchased from now on are changed. The code requires security-by-design principles, zero-trust architectures[10], access restrictions, background checks of supplier personnel where the law allows, contractual audit rights, traceability of requirements throughout the product life cycle, and explicit consideration of the risk of dependence on a single supplier. The obligations become binding for procurement processes launched six months after the controls are adopted, and critical-impact entities must also verify critical components through certification or internal assurance mechanisms.

Scope by criticality: designated entities and perimeters of application

No European entity is automatically covered by the code. The national authority designates high-impact and critical-impact entities by applying thresholds derived from an index that measures the effect that compromising the processes the entity operates would have on cross-border electricity flows. The provisional thresholds, published by the European Network of Transmission System Operators together with the EU DSO Entity, are expressed country by country in megawatts and vary considerably according to the size and degree of interconnection of each national system.

Classification does not stop at the entity. Within each designated company, perimeters are defined: the assets needed to run high-impact processes form a perimeter subject to the minimum controls, and those needed for critical-impact processes form a perimeter subject to the advanced controls. The obligation thus targets the set of assets that would cause the damage rather than the company's entire infrastructure, which limits the cost of compliance without reducing protection where it matters.

The mechanism separates the requirement from the size of the company and ties it to the damage its failure would cause: a small distribution utility whose operations prove decisive for a critical process falls within the enforceable perimeter, while a larger company located in a highly redundant area may end up at a lower level. The regulation also provides for limited derogations where the cost of a control is disproportionate and alternative safeguards exist.

Compliance verification and comparative assessment of cost

Verification is organized in cycles. Each designated entity must cover the full verification scope at least once every three years, with annual partial audits, and may demonstrate compliance through a national verification scheme supervised by the authority or through an independent third-party audit, with requirements of independence, sector knowledge, and confidentiality. Critical-impact entities must demonstrate compliance with the controls within twenty-four months of their adoption or update.

On cost, the code entrusts national energy regulators with an unprecedented task: to assess, on a comparative basis, whether the cybersecurity investments of regulated entities are effective, efficient, and integrated into procurement processes. To this end, the European regulators' agency published non-binding methodological guidance in June 2025, and national regulators must carry out the exercise within the following twelve months. The results are confidential and are shared among the competent authorities, the regulators' agency, the cybersecurity agency, and the Commission.

The exercise does not constitute tariff

[10] Zero trust: A security model that does not assume any device, user, or connection is trustworthy simply because it is inside the network, and that requires identity and permissions to be verified at every access.

recognition. Its effect comes earlier and is of a different nature: it requires the regulator to treat the cost of cybersecurity as a category of its own, measurable and comparable across companies, instead of leaving it diluted within general technology spending.

5.3. UNITED KINGDOM: THE ENERGY REGULATOR AS CYBERSECURITY AUTHORITY

The United Kingdom combines two features that rarely coincide: a cybersecurity regime for critical infrastructure and an incentive-based economic regulation framework, both administered by the same body in the distribution segment. The economic framework is RIIO (Revenue = Incentives + Innovation + Outputs), a multi-year price control under which the fourteen distribution network operators submit business plans that the regulator assesses, approves, and translates into allowed revenues, with adjustment mechanisms during the period. The cybersecurity regime derives from the 2018 Network and Information Systems Regulations, which the country retained after leaving the European Union and which assign each sector its own competent authority. The national technical cybersecurity authority provides the assessment framework and doctrine, but does not directly supervise companies in the energy sector.

A single authority and an outcome-based assessment framework

For the downstream gas and electricity segment, which explicitly includes distribution utilities, the competent authority is the energy regulator itself, acting jointly with the relevant government department. The same body that sets the network's remuneration oversees its cybersecurity, so the requirement and its funding are discussed at the same table, with the same case file and under the same reasonableness criterion.

The assessment is based on the Cyber Assessment Framework developed by the national technical authority, organized into four objectives, managing security risk, protecting against cyberattack, detecting cybersecurity events, and minimizing the impact of incidents, fourteen principles, and just over forty contributing outcomes. Each outcome is accompanied by indicators of good practice that describe the evidence supporting a rating of achieved, partially achieved, or not achieved.

The difference from a checklist is substantial: the framework specifies what must be achieved, not what must be installed. This shifts the discussion from an inventory of tools to effectiveness, and allows a small company to achieve an outcome with a simple, well-run architecture without replicating a large group's infrastructure. The energy regulator adapts the framework through a sector profile that defines the expected level by type of entity, and has been tightening specific areas, in particular supply chain security and requirements for critical suppliers.

RIIO: cybersecurity as a tariff line item

The price control currently in force for electricity distribution, which runs from April 2023 to March 2028, separates cybersecurity from the ordinary business plan and gives it its own treatment.

The design has four components. First, companies submit cyber resilience plans differentiated for information technology and operational technology, assessed against minimum quality requirements: funding is tied to a verifiable plan, not to a statement of intent. Second, that plan receives a specific allowance within allowed revenues. Third, there are reopener mechanisms, one for information technology and one for operational technology, that allow the allowance to be adjusted during the price control period when circumstances change, with a limited decision timeframe so that the outcome can be incorporated into the annual revenue

update process. And fourth, the allowance operates as a price control deliverable subject to a use-it-or-lose-it condition: the money recognized for cybersecurity cannot be spent on anything else and, if the committed plan is not delivered, it is returned.

The result is a symmetrical arrangement. The regulator provides funding, but requires a verifiable plan, reserves the right to periodic review, and prevents the allowance from becoming budgetary slack. The reopener, moreover, explicitly recognizes that the threat evolves faster than the regulatory cycle, a mismatch that no fixed-period price control can resolve through forecasting.

The security regime, for its part, is under review: in November 2025, a cyber security and resilience bill was introduced in Parliament that updates the 2018 regulations and expands existing obligations, including on suppliers and managed service providers.

5.4. AUSTRALIA: PROPORTIONALITY AS A DESIGN PRINCIPLE

Australia built its regime on two components that operate on different planes: a cross-sector critical infrastructure law, applicable to a broad set of sectors, and an energy-sector maturity framework developed by the industry itself together with the market operator and government agencies.

The market operator occupies a unique position. In addition to running the wholesale market and operating the system, it acts as coordinator of sector cybersecurity: it convenes the annual assessment exercise, consolidates the results, and publishes the framework and its guidance materials. That dual role explains why the instrument was developed from within the sector rather than imposed from outside, and why it was entirely voluntary during its first years.

The AESCSF: a sector maturity model

The Australian Energy Sector Cyber Security Framework was first published in 2018 and updated in 2022. It was built on existing international capability models and reference frameworks, mainly the U.S. Department of Energy's Electricity Subsector Cybersecurity Capability Maturity Model and the National Institute of Standards and Technology's Cybersecurity Framework, and it refers to general-purpose control standards for technical detail.

The assessment is organized into eleven domains: risk management; asset, change, and configuration management; identity and access management; threat and vulnerability management; situational awareness; information sharing and communications; event and incident response and continuity of operations; supply chain and dependencies management; workforce management; cybersecurity program management; and privacy management in accordance with Australian law. Within each domain, practices are arranged in maturity levels ranging from zero to three.

On that basis, cumulative security profiles are defined. Each higher profile assumes the previous one has been achieved, and each organization's target profile depends on its criticality to the sector, not on its revenue or number of customers. A small company is not exempted: it is placed in a lower profile, with an achievable target and a trajectory comparable to that of the rest. All use the same language, the same measurement instrument, and the same scale, which makes the results aggregable and comparable across organizations and over time.

That last feature explains the framework's origin. It began as a sector self-assessment tool, and for several years the sector measured itself, in an annual cycle coordinated by the market operator, before the law required anything of it. That measurement produced the baseline that later

made it possible to set obligations with realistic levels and dates.

It is worth noting that there is a specific domain devoted to workforce management, which turns the availability of qualified staff into a measured and comparable dimension, rather than an implicit constraint that each company manages on its own.

From voluntary framework to legal obligation: the critical infrastructure law

Australia's Security of Critical Infrastructure Act and its risk management program rules made it mandatory, from August 2024, for responsible entities to adopt a recognized cybersecurity framework; the energy sector framework was accepted as one of them, together with general-purpose international standards.

The regime was substantially tightened in June 2026, when strengthened rules came into force requiring responsible entities in the energy sector to reach the sector framework's second security profile by June 30, 2028, with implementation periods of twelve to twenty-four months for the remaining requirements and with the requirement aligned with the existing annual attestation cycle. The legal obligation does not list controls: it sets a maturity level and a date.

The result is a two-layer model. The general law requires having a recognized framework and reaching a given level within a given deadline; the sector framework, developed with the industry and updated with it, defines how that level is measured. The legislator does not need to write technical controls that will become outdated within a few years, and the discussion with the sector is not about whether it complies, but about how it demonstrates compliance.

The link with economic regulation runs through a less structured route than the British one, but an equally workable one: distribution utilities submit specific business cases to the economic regulator to reach given maturity levels of the sector framework. When the obligation is expressed as a verifiable level with a fixed date, the cost of meeting it becomes something that can be argued within the rate-setting process.

5.5. ONTARIO: MATURITY-BASED REGULATION FOR A DIVERSE SET OF DISTRIBUTORS

The Ontario case is of interest because of the composition of its regulated universe. The provincial energy regulator oversees around sixty local distribution companies, most of them municipally owned and of very different sizes, ranging from companies serving more than a million customers to municipal utilities with a few thousand. It is a sector structure that resembles that of several Latin American countries more than that of any of the other benchmarks reviewed.

The regulatory instrument is also distinctive. The regulator did not need a law: it incorporated the cybersecurity obligations through amendments to the transmission and distribution codes, which are rules within its own remit and form part of the licence conditions. This allowed it to act quickly and adjust its approach over time without opening a legislative process.

In 2018, those amendments required licensed transmitters and distributors to use a cybersecurity framework developed with the industry and to report the maturity level achieved to the regulator. The framework was based on a widely used public capability model, with maturity levels applied to the functions of identify, protect, detect, respond, and recover, and it also included a privacy dimension.

The reporting mechanism is its most distinctive feature: an annual self-certification of the maturity level achieved, signed by the company's chief executive and submitted to the regulator. It does not require the authority to set up a body of inspectors

specialized in industrial security, a capability that is expensive, scarce, and hard to retain in any public administration, and it produces an effect that no external audit achieves as economically: it forces the issue to reach the company's highest decision-making level at least once a year, with a personal signature involved.

In October 2024, a mandatory cybersecurity standard came into force, replacing the declarative approach with enforceable requirements. The full sequence, six years of measurement and reporting before the obligation, was not a delay but the building of the two conditions that make a mandatory rule viable: that the regulator knows where its sector really stands, and that companies have their own baseline from which to plan.

5.6. INDIA: REGULATING A LARGE-SCALE SYSTEM WITH UNEVEN MATURITY

India regulates the world's largest power system by number of connections, with state-owned, private, and mixed distribution utilities of very uneven financial and technical performance. The Central Electricity Authority, the federal government's technical body, has the power to issue rules applicable to the entire sector, and it has used that power to put cybersecurity obligations in place without waiting for companies to reach a homogeneous level of maturity.

The path went from lesser to greater enforceability. The authority first issued cybersecurity guidelines for the power sector and then moved toward a sector regulation, whose draft was submitted for public consultation in October 2025. The proposed scope covers generation, transmission, and distribution, and extends to power exchanges, load dispatch centers, and suppliers of information and control systems, so the obligation does not stop at the regulated company but reaches those who supply the technology with which it operates.

The obligations are markedly prescriptive on governance, in contrast with the British outcome-based approach and the Australian maturity-based approach: appointment of a chief information security officer and an alternate, both from senior management and reporting to the highest level of the organization; an information security division operating around the clock; mandatory audits by accredited auditors; and requirements on the control systems supply chain.

The institutional component is the most distinctive feature of the case. India has an incident response team specific to the power sector, which acts as the central agency for reporting, response, and analysis and works in coordination with the national team. The existence of that single point turns mandatory reporting into an exchange: the company that reports receives alerts, analysis, and coordination in return, and the authority builds up an aggregate view of the threat that no individual company could build on its own.

5.7. MECHANISMS THAT INTERNATIONAL EXPERIENCE PUTS ON THE TABLE

The six cases above lend themselves to a cross-cutting reading that organizes the experience not by jurisdiction but by the design problem each instrument solves.

Scope: how to define who is covered

Four inclusion criteria can be observed. The first is impact on the system, measured with a common index and expressed as country-specific thresholds, as in the European Union: it is the most precise and the most demanding in terms of information. The second is the classification of assets by criticality, as in the United States: it defines not which companies are covered but which requirements apply to each asset. The third combines segment and

number of regulated customers, and is the criterion found in the most recent sector regulations, including the one being drafted in Chile. The fourth is administrative designation by class of critical asset, as in Australia. To these is added, in Ontario, the simplest route of all: the sector licence, which brings in the entire regulated universe without exception.

Inclusion criterion	Where it applies	Covers distribution?	Information required of the regulator
Impact on the system, with country-specific thresholds	European Union	Yes, if it exceeds the threshold	High: requires modeling the systemic impact of each operator
Asset criticality (high / medium / low)	United States	Only bulk power system assets	Medium: asset inventory and classification
Segment and number of regulated customers	India; regulation being drafted in Chile	Yes, explicitly	Low: information already available to the regulator
Administrative designation by class of critical asset	Australia	Yes	Medium: legal definition of asset classes
Sector licence (all licensees)	Ontario	Yes, with no size exemption	Low: the universe is the licence register

Table 5.1. Criteria for defining the obligated universe and the information they require.

Requirements: prescriptive controls, management systems, or assessed maturity

The three models coexist and are not mutually exclusive. Prescriptive controls, the standard that lists what must be implemented, are easier to audit than any other model, but they age quickly and disproportionately penalize small companies, which must implement the same things with fewer resources. A management system shifts the burden of proof to the company and adapts to different sizes, but runs the risk of becoming paper compliance. Assessed maturity follows a trajectory rather than setting a binary threshold, is the best fit for a heterogeneous sector, and is also the most demanding for the regulator, because assessing maturity requires technical judgment and not just verification.

The most advanced jurisdictions combine them. The United Kingdom assesses outcomes and funds a plan. Australia layers a law that requires reaching a level on top of a sector framework that defines how it is measured. The European Union requires a management system with controls differentiated by impact level and periodic verification. The combination, rather than the choice among models, is what characterizes mature frameworks.

Funding: who pays and with what instrument

This is where international experience is scarcest. Four instruments can be identified, from greater to lesser institutional complexity.

1. Dedicated tariff allowance with reopeners and a use-it-or-lose-it condition (United Kingdom). It is the most complete design. It requires a multi-year price control with adjustment mechanisms within the period.

2. Regulatory asset with deferral and return (United States). Its lack of use is a warning about calibration: the benefit must comfortably exceed the cost of applying for it.

3. Comparative assessment of the efficiency of investments (European Union). It is the cheapest step and the only one that does not require changing the tariff framework: it only requires measuring the cost of cybersecurity as

a separate category and comparing it across companies.

4. Business case before the economic regulator (Australia). It works where the tariff framework already allows investment plans to be submitted for discussion, and it relies on the obligation being expressed as a verifiable level with a date.

The most important observation is that none of these four instruments is part of the security regulation: all of them are developed in economic regulation. Sector regulation defines what must be done; the remuneration framework defines whether it can be done.

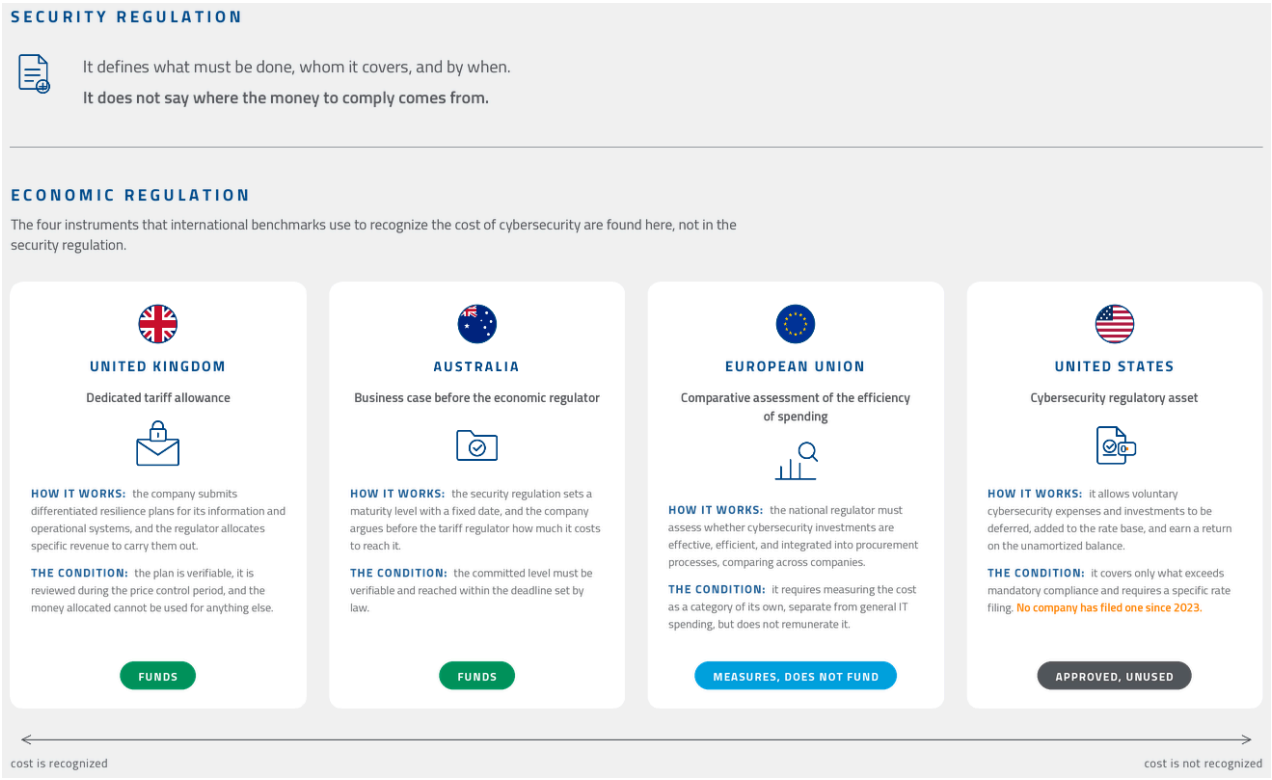


Fig. 5. How cybersecurity is funded: four international instruments

Proportionality: how the cooperative coexists with the large group

All the jurisdictions reviewed solved this problem through scaling instruments, and none did so by exempting small companies.

The last row deserves emphasis. All jurisdictions use time as a proportionality tool: deadlines of thirty-six and sixty months depending on asset criticality in the United States; twelve and twenty-four months depending on impact level in the European Union; windows of twelve to twenty-four months and a sector target set for 2028 in Australia. Differentiating deadlines requires no methodological sophistication and delivers much of the proportionality effect being sought.

Incident reporting and coordinated response

All the jurisdictions reviewed have mandatory incident reporting with short deadlines, and all pair it with two elements: a sector channel for response and analysis, and explicit rules on the confidentiality and anonymization of the information shared. Reporting without protection for the reporter produces fewer reports, not fewer incidents.

A detail of the U.S. case sheds light on the point from another angle. Of the only two items included in the list of pre-approved investments for the rate incentive, one is participation in the threat information sharing program. In other words, the jurisdiction that most heavily penalizes non-compliance also decided to fund participation in the information sharing mechanism.

Technique	Jurisdiction	How the level is determined	What is required of the smallest company
Impact thresholds on the system	European Union	Common impact index, with national thresholds in MW	Nothing, if below the threshold; full minimum controls, if above it
Asset impact levels	United States	Categorization of the cyber system as high, medium, or low	Reduced requirements, proportional to the asset it operates
Cumulative security profiles	Australia	The entity's criticality to the sector	Reach the first profile, with a fixed date and a defined trajectory
Sector profile of the assessment framework	United Kingdom	Type of entity, defined by the energy regulator	Demonstrate security outcomes, not implement identical controls
Self-certified maturity levels	Ontario	Annual self-assessment against the common framework	Declare its actual level and its improvement plan, signed by the chief executive
Differentiated deadlines	All	Criticality of the asset or type of entity	More time to reach the same target

Table 5.2. Proportionality techniques observed in international experience.

5.8. TAKEAWAYS FOR LATIN AMERICA

The preceding comparison reveals an asymmetry worth stating before any transfer. International experience offers abundant and proven answers on what to require and how to scale requirements, and scarce answers on how to fund them. The two most complete ones, the British and the American, come not from security regulations but from economic regulation frameworks, and the second has not even been used.

Three conditions that the benchmarks take for granted are not guaranteed in the region. The first is a regulator with its own technical capacity, or stable access to it, to assess maturity in industrial security: without that capacity, any rule degrades into document checking. The second is an operational national cybersecurity agency, with an incident response team, that receives reports and returns analysis and coordination; without it, mandatory reporting is a burden with nothing in return. The third is a tariff framework with periodic reviews and room for new line items: without it, the funding discussion has nowhere to take place. Recognizing these conditions does not invalidate the transfer of the mechanisms; it defines their sequence.

With that caveat, six elements of international experience are applicable in the short term and at low regulatory cost.

1. **Measure before requiring.** Australia and Ontario built their mandatory regimes on several years of prior measurement, and it was that measurement that later made it possible to set realistic levels and dates. The benchmarking on which this document is based is exactly that first step; keeping it going periodically is the cheapest regulatory investment available.

2. **Adopt a maturity framework as a common sector language.** There is no need to create a new one: the Australian, Canadian, and British frameworks are public and rely on freely available capability models. What is transferable is the

decision to adopt one as a reference, which is also what makes results comparable across companies and countries.

3. **Annual self-certification signed by the chief executive.** It is the mechanism with the best ratio of regulatory cost to governance effect in the entire repertoire reviewed, and it does not require building technical enforcement capacity.

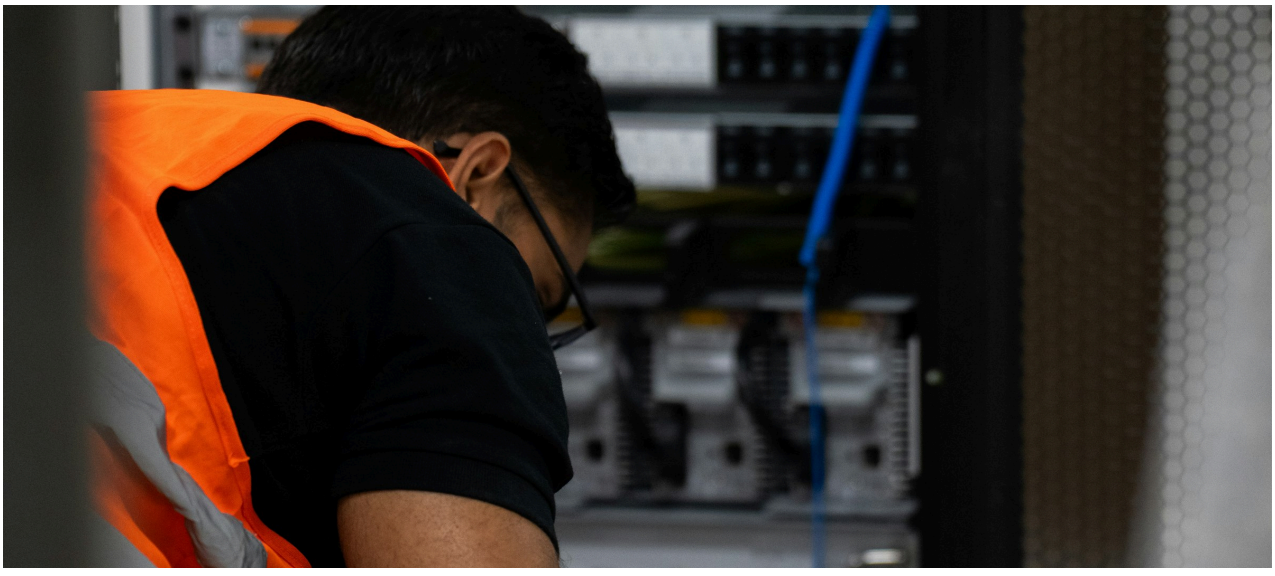
4. **Separate the enabling regulation from the sector standard.** This allows the regulation to require reaching a level by a date, while the technical detail is updated with the industry without the need to amend it.

5. **Build cybersecurity into procurement conditions.** Requiring security by design, credential management, and contractual audit rights in new acquisitions avoids the financially unmanageable problem of retrofitting an installed fleet.

6. **Measure the cost of cybersecurity as a separate category.** It is the prerequisite for any discussion of tariff recognition, does not require changing the remuneration framework, and can begin with the information companies already produce.

Three other elements, by contrast, are not directly transferable. The U.S. enforcement model presupposes an audit and enforcement apparatus that would take years to build and whose cost is hard to justify for the distribution segment. The European impact index requires modeling each operator's systemic effect on system flows, a capability that is not widely available today; the realistic short-term scope criteria are the classification of assets by criticality and the combination of segment with number of regulated customers. And the British tariff mechanism depends on a multi-year price control with reopeners within the period: what is transferable is not its form but its principle, that is, a separate allowance tied to a verifiable plan, reviewable during the period, and ring-fenced.

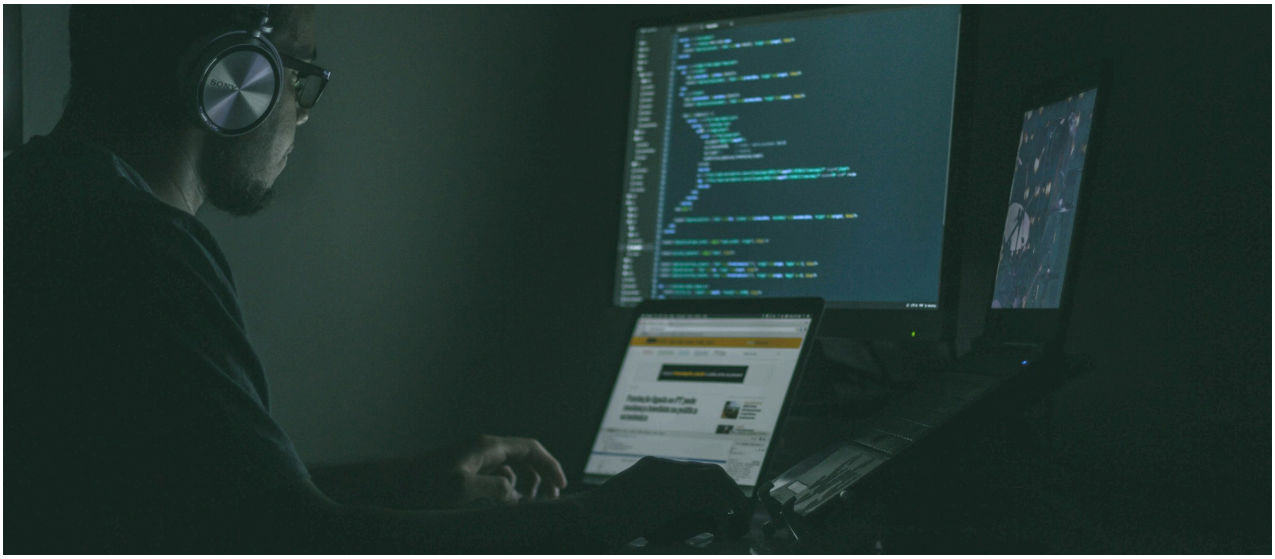
Finally, there remains a decision that international experience does not resolve, because it admits two equally defensible answers. Australia and Ontario measured for years before imposing requirements; India regulated without waiting for maturity, betting that the obligation would generate the capacity. The choice between the two is not technical but political, and it depends on the urgency perceived by the regulator and on how much support it is willing to provide during the transition. The recommendations in the next chapter build on that repertoire.



06

CONCLUSIONS AND REGULATORY RECOMMENDATIONS

The energy transition that regulation promotes is, in practice, a digital transition, and every device connected to the grid expands the surface that must be protected. The evidence gathered by the regional benchmarking, covering twenty-five distribution utilities in ten countries, showed that the sector is already responding to that exposure, and doing so with a pattern that repeated itself across the five dimensions examined: the operational infrastructure, detection and response capability, third parties and data, people, and governance. That progress, however, is not uniform, and the line that divides it is economic rather than technical: progress is made where protection takes the form of investment in assets, the capital expenditure that tariff frameworks know how to incorporate into the remuneration base, and it lags where it requires permanent operating expenditure: daily monitoring, the verification of third parties, staff training, and the specialists who must be retained. The review of Latin American regulation confirmed the other half of the problem because, in the eleven frameworks examined, that expenditure does not exist as a recognized category in the tariff, and companies must fund it from line items designed for other purposes. International experience, for its part, teaches that the requirement and its funding are a single design problem: where the obligation arrived without a way to pay for it, compliance stalled; where the incentive was poorly calibrated, as with the U.S. regulatory asset that no company has applied for, it remained on paper and unused; and where both were designed together, as with the British tariff allowance conditioned on a verifiable plan, protection stopped competing for resources with the rest of the budget. What follows from this review is that the underlying problem is not technical but one of regulatory design, and that until it is corrected, the level of protection of each grid will continue to depend on each company's conviction and financial headroom. Reversing that outcome is not a matter of choosing between requiring and funding, but of doing both within a single design, because an obligation without a funding path produces non-compliance, and funding without an obligation does not guarantee protection.



The joint design begins with the requirement. Comparative experience shows that in sectors where large groups with millions of customers coexist with rural cooperatives of very different economic means, a severe and uniform rule penalizes the small player and may push it to seek to fall outside the rule's scope rather than to protect itself better. The frameworks that have best resolved this heterogeneity, the Australian, the British, and Ontario's, share two decisions: they scale requirements according to the criticality of each operation rather than the size of each company, and they separate the enabling regulation, which sets the level to be reached and its deadline, from the technical standard that defines how to measure it, so that small and large companies move along the same scale at different but verifiable speeds, and the technical detail is updated with the industry without the need to amend the law. Funding, for its part, should be defined as the set of mechanisms for justifying, supervising, and verifying the investments that actually reduce operational risk. The available international repertoire moves from lesser to greater institutional complexity: measuring the cost of cybersecurity as a separate category, which does not require changing the tariff framework and gives the regulator the information it currently lacks; accepting business cases before the economic regulator to reach defined maturity levels; and establishing a dedicated tariff allowance conditioned on a verifiable plan, with periodic review and the return of any unspent funds.

There is a third front that does not require tariff reforms, because it depends on decisions the regulator can take directly with its own instruments: the common infrastructure on which all defense depends. The first component is mandatory incident reporting, whose design matters as much as its existence, because if notifying automatically exposes the reporter to a penalty, the rational incentive is to conceal. Reporting must be accompanied by confidentiality, anonymization rules, and the principle that good-faith notification does not in itself constitute evidence of negligence, a principle that Ecuador's 2026 legislation has already incorporated and that shows the region is in a position to adopt it. The second component is coordinated response. A successful attack against a distribution utility is not an individual problem, because the interdependence of the electricity ecosystem allows the compromise of one link to spread along the chain. In the face of threats that operate on a transnational scale, information sharing and a sector response team raise the capability of all companies without each one having to build it separately, and that space is almost empty in the region today, with only one formalized electricity CSIRT. The third component returns to the origin of the problem, because the same smart metering, remote control, and automation plans that regulators promote and approve can incorporate security as a design requirement, in procurement conditions and in project approval, so that modernization does not keep expanding the exposed surface faster than it is protected.

Companies, for their part, do not need to wait for regulation to move forward, and the diagnosis itself shows that they have already begun. Measuring themselves periodically is the first task, because the maturity regimes operating around the world today were built on years of prior sector measurement, and that path has already been started in the region with exercises such as the one underpinning this diagnosis. What comes next is adopting a public maturity framework as a common language, which allows each company to set itself a target level and demonstrate its progress; bringing cybersecurity into corporate governance, with an officer who has direct access to senior management, a dedicated budget line, and risk expressed in economic terms, which is the language in which boards make decisions; contractually securing every new purchase, requiring security by design and audit rights, so that the fleet being installed today does not

repeat the vulnerabilities of the one installed yesterday; and jointly addressing the shortage of specialized talent, which is a market problem rather than a problem of each company. None of this replaces the regulator's task, but it makes it easier, because a sector that measures itself, governs itself, and demonstrates its progress makes the spending it asks to have recognized verifiable. Ultimately, the pending decision is a simple calculation, because regulating and funding grid protection costs less today than the incident that protection prevents, and the cost of postponing it does not disappear: it builds up silently and ends up being paid by users, in the form of service interruptions, leaks of their data, or emergency spending.



Fig. 6. Recommendations by implementation complexity.

07

REFERENCES

Adaptix Networks. (2022, July 8). *Filtran datos personales de clientes CFE* [Personal data of CFE customers leaked]. 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* [Normative Resolution No. 964 of December 14, 2021: establishing the Cybersecurity Policy and the minimum cybersecurity requirements for electricity sector agents]. 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* [Order No. 427 of February 17, 2025: setting the schedule for the periodic submission of cybersecurity maturity and risk data by electricity sector agents]. https://www2.aneel.gov.br/cedoc/dsp2025427.pdf

Argentina. (2000). *Ley 25.326: Ley de protección de datos personales* [Law 25,326: Personal Data Protection Law]. Agencia de Acceso a la Información Pública.

Argentina. (2017). *Decreto 577/2017: Comité de Ciberseguridad* [Decree 577/2017: Cybersecurity Committee]. 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* [Administrative Decision 641/2021: minimum information security requirements for national public sector bodies]. Boletín Oficial. https://www.boletinoficial.gob.ar/detalleAviso/primera/246104/20210628

Argentina. (2025). *Decreto 941/2025: creación del Centro Nacional de Ciberseguridad* [Decree 941/2025: creation of the National Cybersecurity Center]. InfoLeg. https://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=422011

Asamblea Legislativa de El Salvador. (2025, April 30). *Transferencia de recursos permitirá funcionar la Agencia de Ciberseguridad del Estado* [Transfer of resources will allow the State Cybersecurity Agency to operate]. https://www.asamblea.gob.sv/node/13555

Biblioteca del Congreso Nacional de Chile. (n.d.). *LeyChile* [Legal database]. https://www.bcn.cl/leychile/

Bolivia. (1997). *Código Penal, capítulo XI: delitos informáticos* [Penal Code, chapter XI: computer crimes]. https://www.minsalud.gob.bo/images/Documentacion/normativa/LEY%201768%20CODIGO%20PENAL.pdf

Bolivia. (2013). *Decreto Supremo n.º 1793: reglamento de la Ley n.º 164* [Supreme Decree No. 1793: regulations implementing Law No. 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* [Provision 1/2026: technical regulation on contingency plans and alternative data processing centers]. https://www.argentina.gob.ar/normativa/nacional/disposici%C3%B3n-1-2026-425749/texto

CERT-PY. (2025). *Marco legal: Decreto n.º 3900/2025 y Resolución MITIC n.º 259/2025* [Legal framework: Decree No. 3900/2025 and MITIC Resolution No. 259/2025]. https://www.cert.gov.py/marco-legal/

CERT-UA. (2022, April 12). *Kiberataka hrupy Sandworm (UAC-0082) na obiekty enerhetyky Ukrainy z vykorystanniam shkidlyvykh prohram INDUSTROYER2 ta CADDYWIPER* [Cyberattack by the Sandworm group (UAC-0082) on energy facilities in Ukraine using the INDUSTROYER2 and CADDYWIPER malware] (CERT-UA#4435). https://cert.gov.ua/article/39518

Cherepanov, A. (2017). *Win32/Industroyer: a new threat for industrial control systems* [Technical report]. 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* [Law No. 21,663: Framework Law on Cybersecurity and Critical Information Infrastructure]. 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* [Law No. 21,719: regulating the protection and processing of personal data and creating the Personal Data Protection Agency]. 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* [Supreme Decree No. 295: regulations on the notification of cybersecurity incidents under Law 21,663; early warning within 3 hours; report or update within 72 hours, or 24 hours for operators of vital importance with affected service; final report within 15 days]. 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* [CREG Resolution 101 001 of 2022: advanced metering (AMI), cybersecurity, and 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)* [CREG Resolution 701 11 of 2022: rationale for the prohibition on passing meter costs through to tariffs (Art. 56 of Law 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. (n.d.). *Iniciativa de Ley n.º 6347: Ley de ciberseguridad* [Bill No. 6347: Cybersecurity Law]. 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* [Opinion 01-2025 on Bill No. 6347]. https://www.congreso.gob.gt/assets/uploads/comisiones/dictamenes/97fef-dictamen-6347-fav-casn.pdf

Consejo Nacional de Operación. (n.d.). *Acuerdo CNO 2088: procedimiento y formato de reporte de incidentes, CSIRT sectorial eléctrico y MISP* [CNO Agreement 2088: incident reporting procedure and format, electricity-sector CSIRT, and MISP]. https://www.cno.org.co/content/acuerdo-2088-por-el-cual-se-aprueba-el-procedimiento-y-formato-de-reporte-de-incidentes

Consejo Nacional de Operación. (n.d.). *Acuerdos* [Agreements; compilation: 788/2015, 1241/2019, 1347/2020, 1463/2021, and 1502/2021]. https://www.cno.org.co/calendar-acuerdos

Consejo Nacional de Operación. (n.d.). *Ciberseguridad* [Cybersecurity; web page of the cybersecurity committee]. https://www.cno.org.co/content/ciberseguridad-7

Consejo Nacional de Operación. (2025). *Acuerdo CNO 1960 de 2025: actualización de la Guía de ciberseguridad con enfoque basado en riesgo* [CNO Agreement 1960 of 2025: update of the Cybersecurity Guide with a risk-based approach]. 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, November 15). *Decretos n.º 143 y n.º 144* [Decrees No. 143 and No. 144]. https://transparencia.mh.gob.sv/downloads/pdf/700-UAIP-LY-2024-14993.pdf

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

El Deber. (2026, January 14). *El Gobierno reordena la firma digital y saca a la ADSIB de la Vicepresidencia* [The government reorganizes digital signatures and moves ADSIB out of the Vice Presidency]. 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* [Legislative Decree No. 143: Cybersecurity and Information Security Law]. Refworld. https://www.refworld.org/es/leg/legis/pleg/2024/149335

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

FUNDESA. (n.d.). *Ley de ciberseguridad debería regresar a la Comisión* [Cybersecurity law should go back to committee]. https://fundesa.org.gt/en/publications/opinion/ley-de-ciberseguridad-deberia-regresar-a-la-comision

Gobierno de Colombia. (2022). *Decreto 338 de 2022: crea colCERT, CSIRT Gobierno, CSIRT Defensa y la Plataforma Nacional de Notificación y Seguimiento de Incidentes* [Decree 338 of 2022: creating colCERT, CSIRT Government, CSIRT Defense, and the National Incident Notification and Tracking Platform]. https://normograma.mintic.gov.co/mintic/compilacion/docs/decreto_0338_2022.htm

InfoLeg. (n.d.). *Compilado de normativa de ciberseguridad* [Compilation of cybersecurity regulations]. https://servicios.infoleg.gob.ar/infolegInternet/anexos/365000-369999/365238/norma.htm

La República. (2022, August 22). *Ley de ciberseguridad* [Cybersecurity law]. https://www.larepublica.net/noticia/ley-de-ciberseguridad

La Tercera. (2019). *Gobierno argentino cree que apagón no fue un ciberataque pero no lo descarta* [Argentine government believes the blackout was not a cyberattack but does not rule it out]. https://www.latercera.com/mundo/noticia/gobierno-argentino-cree-apagon-no-fue-ciberataque-no-lo-descarta/702370/

Lee, R. M., Assante, M. J., & Conway, T. (2016). *Analysis of the cyber attack on the Ukrainian power grid* (ICS Defense Use Case No. 5). SANS Industrial Control Systems & 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, November 14). *Se aprueba la Ley para la protección de datos personales y la Ley de ciberseguridad y seguridad de la información* [Personal Data Protection Law and Cybersecurity and Information Security Law approved]. 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* [Costa Rica's National Cybersecurity Strategy 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. (n.d.). *Poder Ejecutivo oficializa la Estrategia nacional de ciberseguridad 2025-2028* [Executive branch makes the 2025-2028 National Cybersecurity Strategy official]. https://mitic.gov.py/enc2025-2028/

Ministerio de Tecnologías de la Información y Comunicación. (2025). *Estrategia nacional de ciberseguridad de Paraguay 2025-2028* [Paraguay's National Cybersecurity Strategy 2025-2028]. https://mitic.gov.py/eoj0cad9uplo/2025/05/ENC-Paraguay-2025-2028-Mayo-20251558.pdf

Osinergmin. (2014). *Resolución n.º 270-2014-OS/CD: estándares técnicos mínimos* [Resolution No. 270-2014-OS/CD: minimum technical standards]. 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

Paraguay. (2020). *Ley n.º 6534/2020: Ley de protección de datos personales crediticios* [Law No. 6534/2020: Credit Personal Data Protection Law]. 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* [Law No. 29733: Personal Data Protection Law]. 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* [Emergency Decree No. 007-2020: digital trust framework]. https://www.gob.pe/institucion/pcm/normas-legales/395322-007-2020

Peru. (2024, February 14). *Decreto Supremo n.º 017-2024-PCM: reglamento de la Ley de Ciberdefensa* [Supreme Decree No. 017-2024-PCM: regulations implementing the Cyber Defense Law]. El Peruano. https://www.congreso.gob.pe/Docs/DGP/DIDP/files/ds_017-2024-pcm.pdf

Peru. (2025, November 4). *Decreto Supremo n.º 126-2025-PCM: reglamento del Decreto de Urgencia n.º 007-2020* [Supreme Decree No. 126-2025-PCM: regulations implementing Emergency Decree No. 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* [Resolution 829/2019: National Cybersecurity Strategy]. Boletín Oficial. https://www.boletinoficial.gob.ar/detalleAviso/primera/208317/20190528

Secretaría de Gobierno de Modernización. (2019). *Resolución 1523/2019: definición de infraestructuras críticas* [Resolution 1523/2019: definition of critical infrastructure]. Boletín Oficial. https://www.boletinoficial.gob.ar/detalleAviso/primera/216860/20190918

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


adelat