

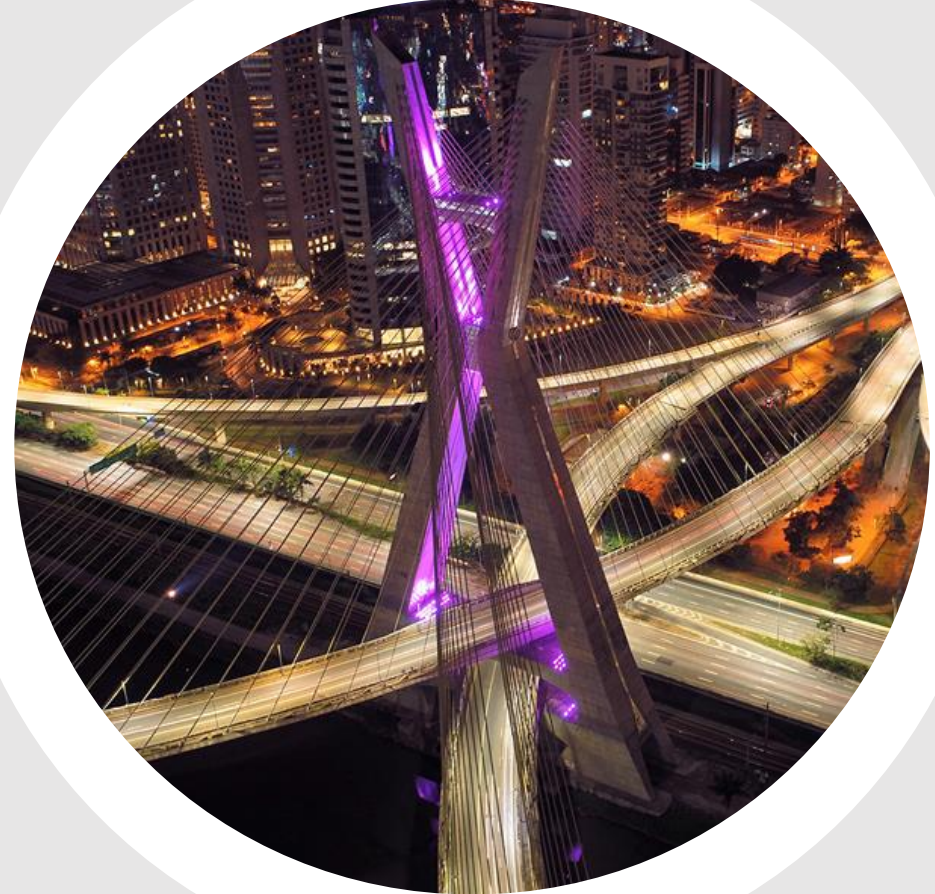






ccee

Câmara de Comercialização  
de Energia Elétrica

# Commercialization of Electric Energy

OCTOBER/2022

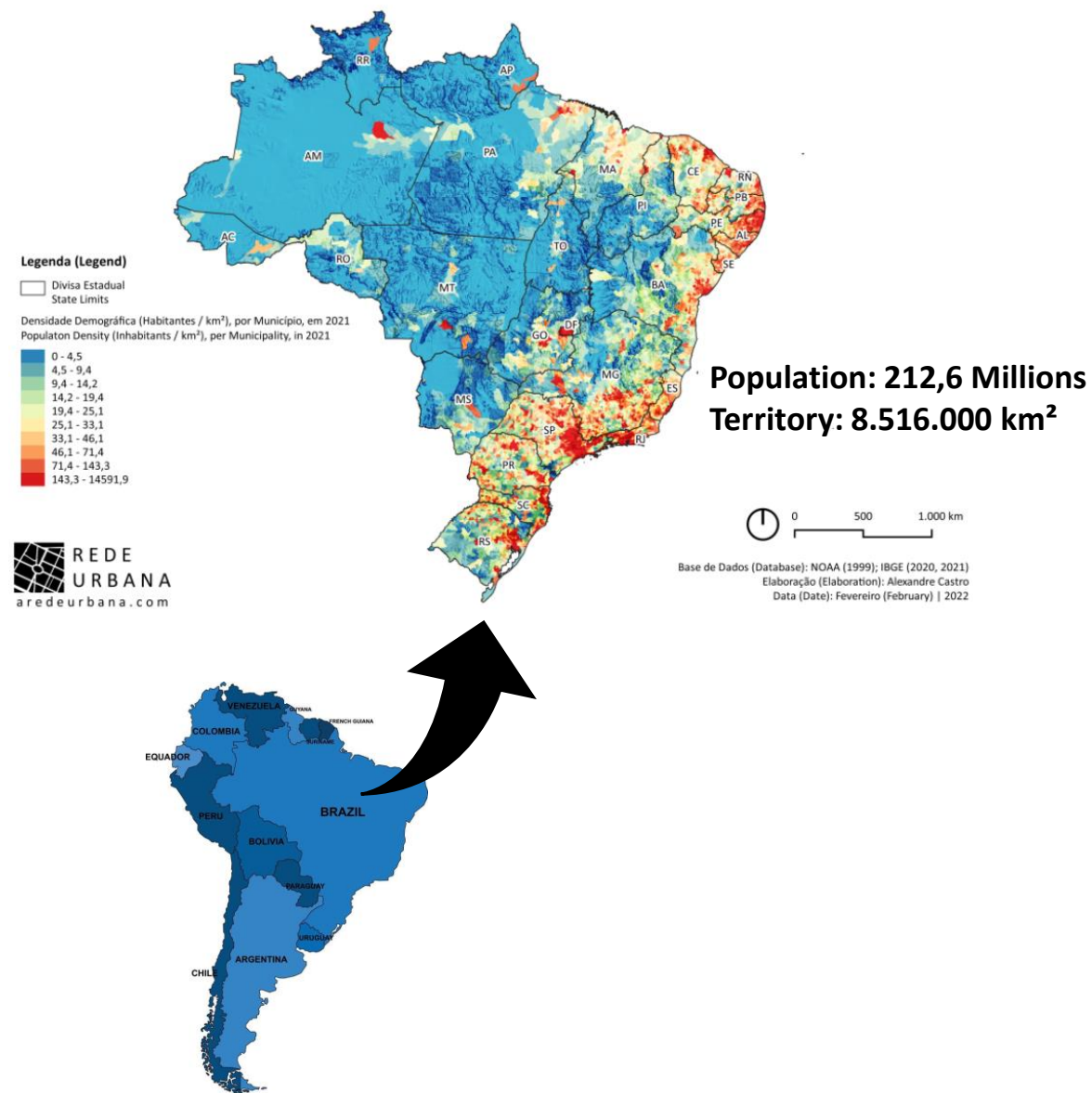


01	Brazilian Electrical Sector and CCEE	
02	Regulations and Processes	
03	Technology	
04	Difficulties and Challenges	





## POPULATION DENSITY OF BRAZILIAN MUNICIPALITIES (2021)





Created in 1999, CCEE is a private, non-profit institution that brings together all companies that sell electricity in Brazil

## Purpose

Develop efficient, innovative and sustainable energy markets for the benefit of society

## Vision 2030

To be a world reference in the operation of energy markets

## OUR VALUES



Collaboration



Commitment to the  
Customer



Ethics and Transparency



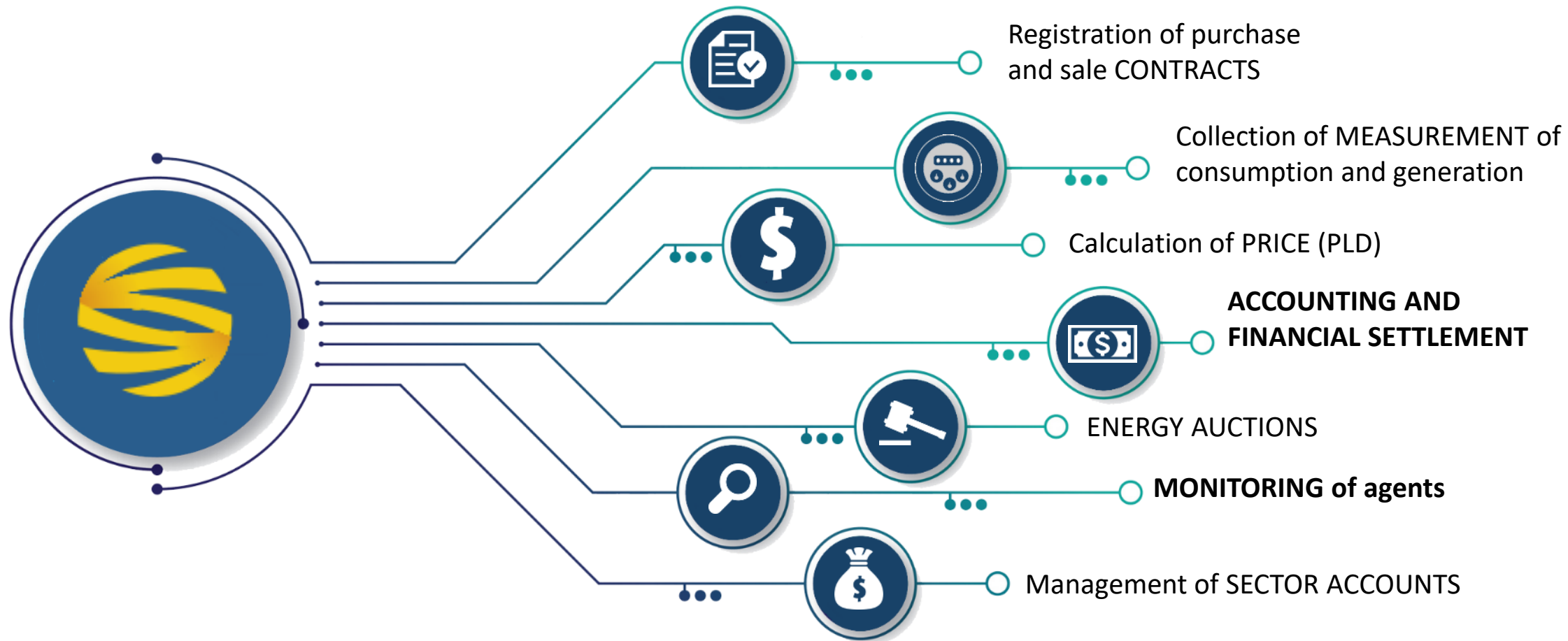
Excellence



Appreciation of People







Customer  
Service



Technology  
and Systems

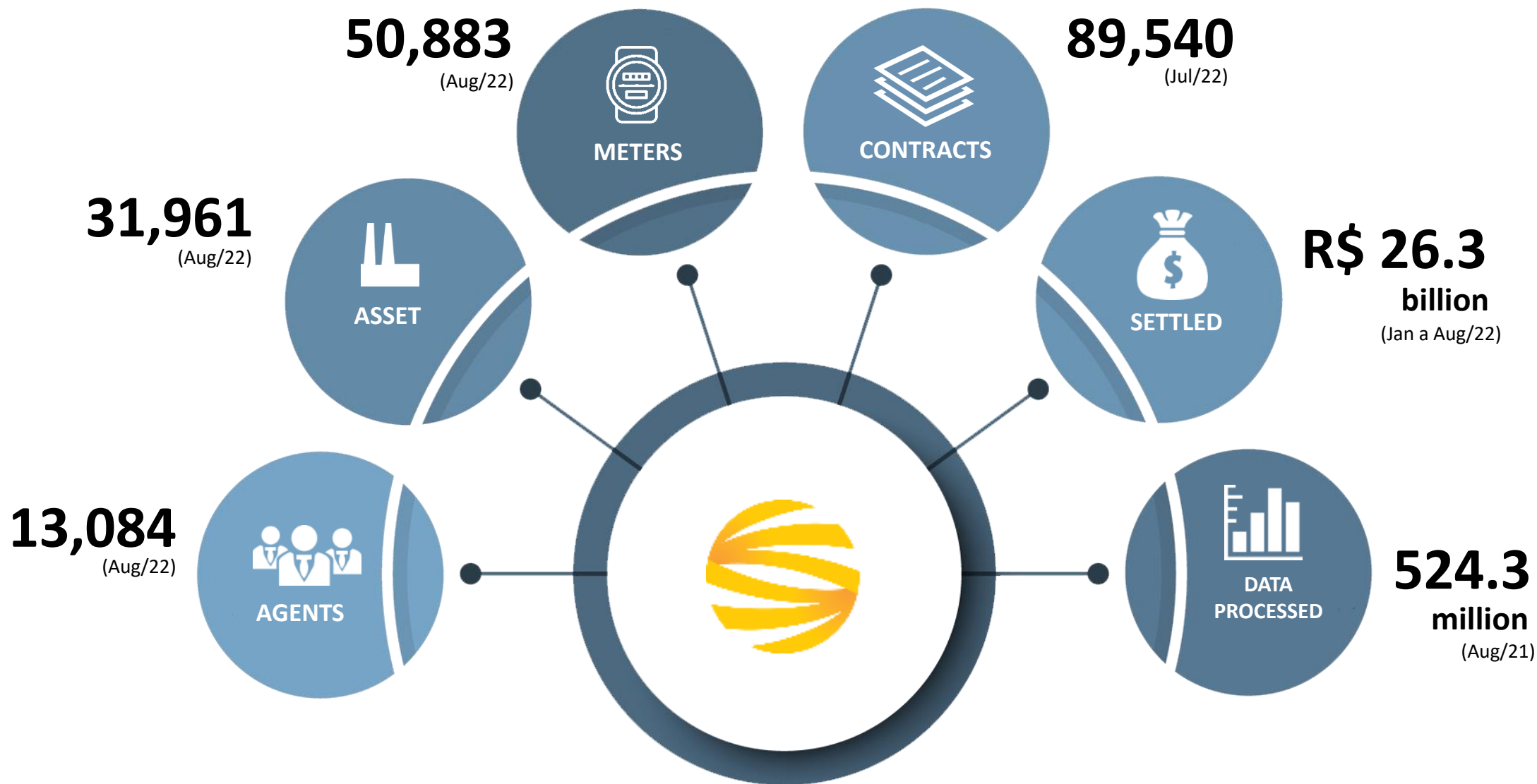


Training



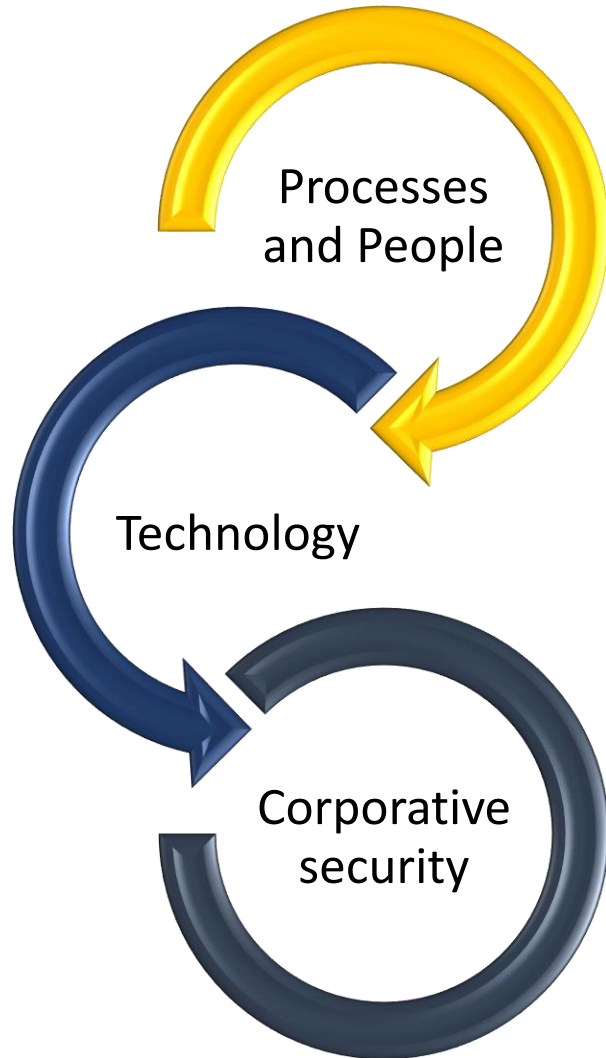
Marketing Rules





2014	04/23	Law 12,965	Civil Rights Framework for the Internet
	08/14	Law 13,709	<b>General Personal Data Protection Act</b> (Driver's Privacy Protection Act)
2018	11/22	Presidential Decree 10,748	Establishes the <b>Federal Cyber Incident Management Network</b>
	12/26	Presidential Decree 9,637	which established the <b>National Information Security Policy</b> , within the scope of the Federal Public Administration
2021	06/01	Resolution 4,658, of Cons. National Monetary Fund, and Circ. 3,909, of BC	provides for <b>cyber security policy</b> and requirements for contracting <b>cloud data</b> processing and storage services
	06/16	Presidential Decree 9,573	Establishes the <b>National Critical Infrastructure Security Policy</b>
	06/16	Presidential Decree 10,748	Establishes the <b>Federal Cyber Incident Management Network</b>
	10/24	ANEEL Resolution No. 24	Approves the <b>Guidelines on Cyber Security for the Electricity Sector</b> , as established in CNPE Resolution No. 1, of February 10, 2021, considering the aspects of prevention, treatment, response and systemic resilience.
	12/14	ANEEL Resolution No. 964	Provides for the <b>Cyber Security Policy</b> to be adopted by agents in the electricity sector



**GEGOI - Executive Management of Institutional Governance**

Processes, Policies and Standards

Security Training Programs

Prior security and privacy assessment of third-party applications

**TM - Market Technology**

Recognized technologies in the market focused on cybersecurity and trained staff

**CCEE**

A stable, secure and available environment for energy trading with transparent cyber barriers preventing / discouraging attacks on infrastructure and services





### Make different

- The use of gamification has clear effects in this context
- Hands on training based on our business
- Hybrid work first, has new challenges and people have less time now and courses must be limited to an one hour.

### Engage Managers

- Management is responsible for strengthening the motivation and security culture and includes the adaptation of his processes under aspects of information security.

### Adoption of modular training

- We apply awareness for all entrance employees;
- Security and Privacy protection as a standard for business analyst, ambassadors of privacy, Human resource and communication area.

### Employees have different starting point

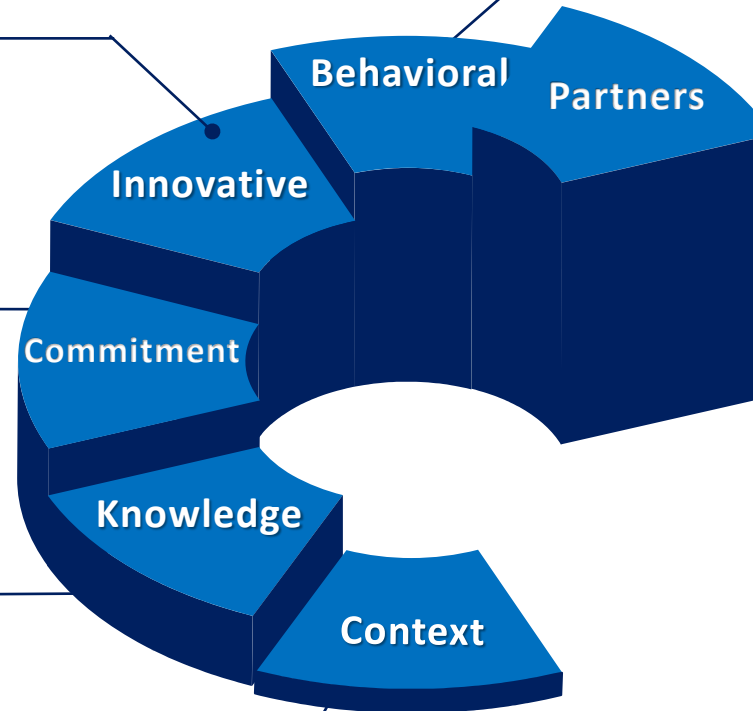
- We personalized learning paths, make what employees have learned tangible and relevant.
- We seek to understand the individual role, C-Level, managerial positions, privileged access rights or employees in the finance department are different target to attacks.

### Improving behavioral security

- The construction of cybersecurity programs awareness must incorporate privacy principles;
- Investing in security awareness should be seen as an investment in the security of the organization and calculated against the potential costs in the event of damage.

### Increasing resilience

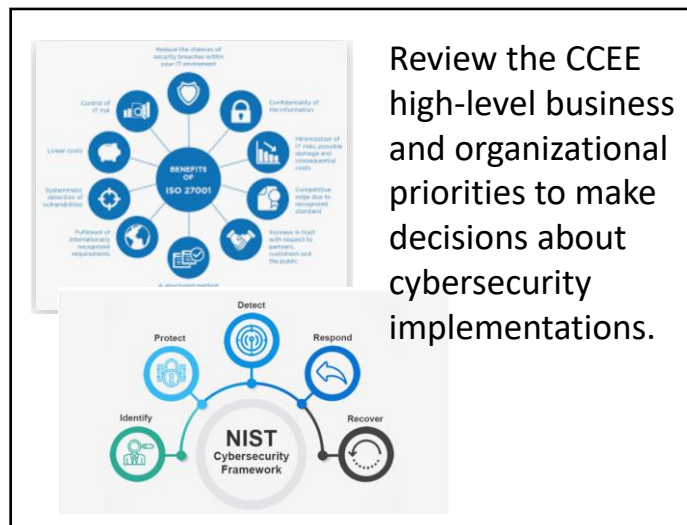
- The CCEE selects its partners and considers the associated risks (trade-off);
- The cybersecurity ecosystem of an organization must maintain a strong culture of security, so connected resilience will be of massive importance.



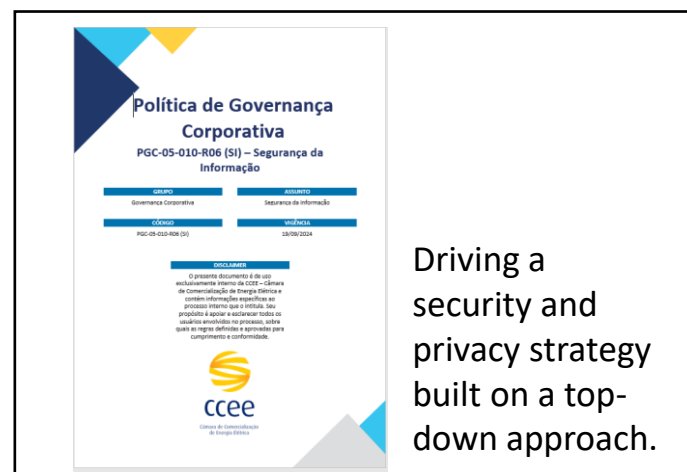
**Employees are an active part of the solution to the cybercrime problem!!!**



## Cybersecurity Framework



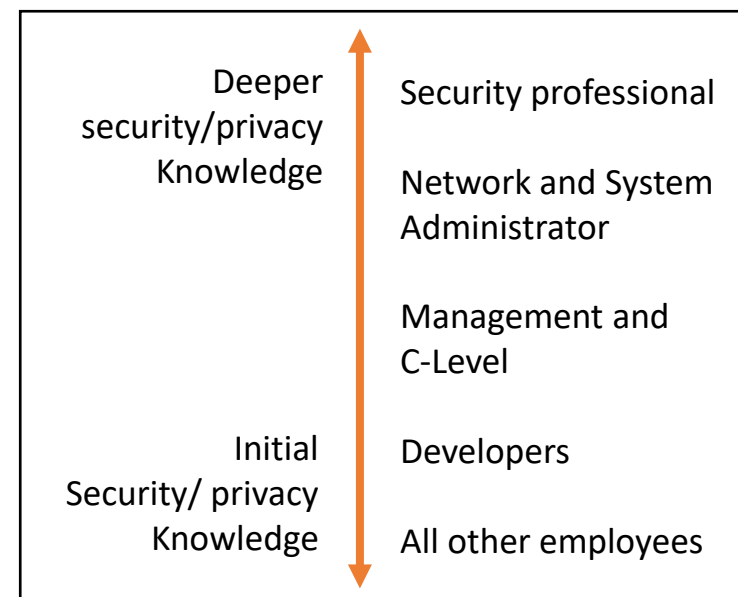
## Cybersecurity guidelines



## Regulatory framework in Brazil

2014	04/23 Law No. 12,965 - Civil Rights Framework for the Internet
	08/14 Law 13.709 - General Personal Data Protection Act (Driver's Privacy Protection Act)
2018	11/22 Presidential Decree 10,748 Establishes the Federal Cyber Incident Management Network
	12/26 Presidential Decree 9,637, which established the National Information Security Policy, within the scope of the Federal Public Administration
	06/01 Resolution 4,658, of Cons. National Monetary Fund, and Circ. 3,909, of BC, provides for cyber security policy and requirements for contracting cloud data processing and storage services
	06/16 Presidential Decree 9,573 Establishes the National Critical Infrastructure Security Policy
2021	06/16 Presidential Decree 10,748 Establishes the Federal Cyber Incident Management Network
	10/24 ANEEL Resolution No. 24 Approves the Guidelines on Cyber Security for the Electricity Sector, as established in CNPE Resolution No. 1, of February 10, 2021, considering the aspects of prevention, treatment, response and systemic resilience.
	12/14 ANEEL Normative Resolution No. 964 - Provides for the Cyber Security Policy to be adopted by agents in the electricity sector

## Who needs to training?



## USERS



Agents



Stakeholders



Consulting



General public

## CHANNELS

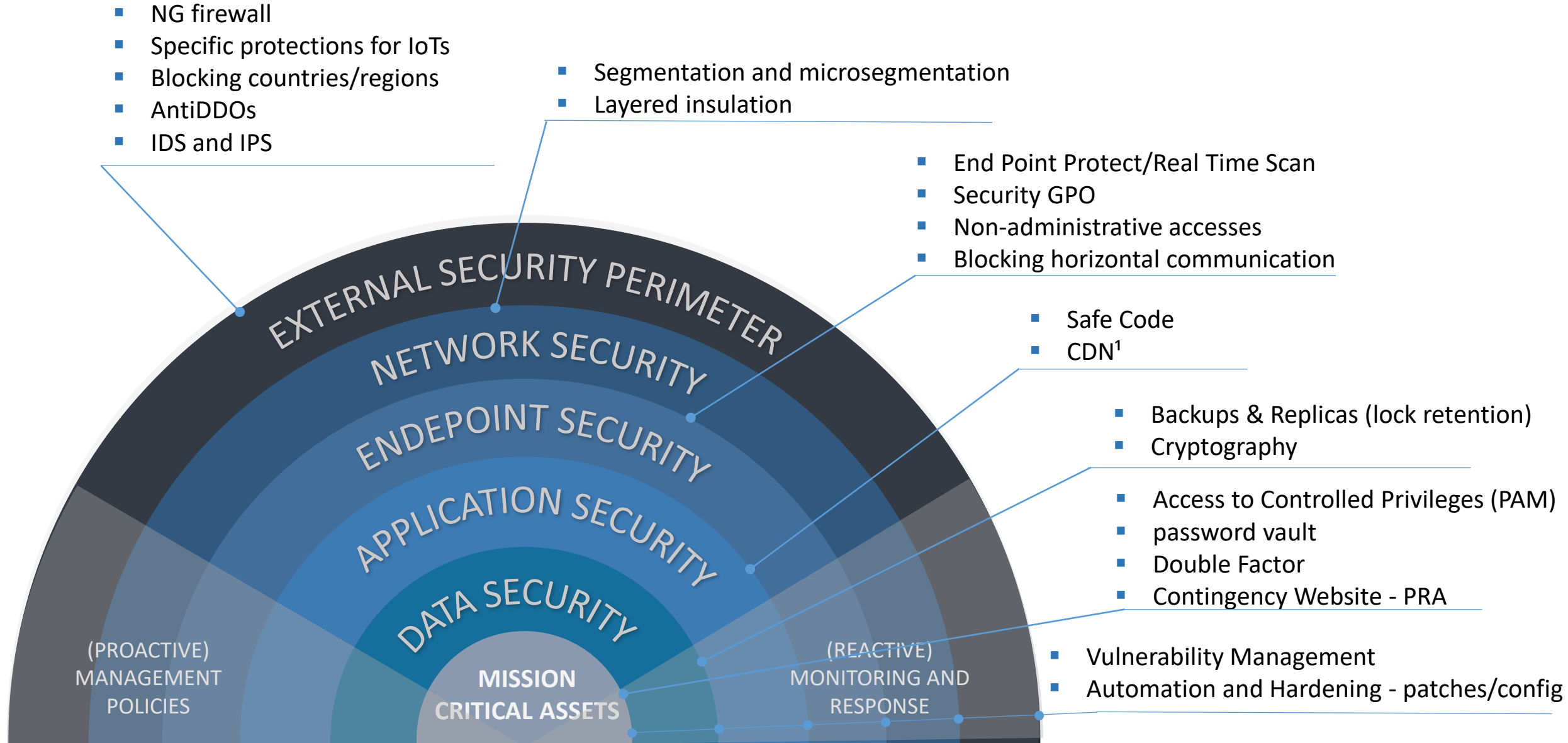
Corporate  
PortalIntegrated  
Environment  
of OperationIntegration  
PlatformMobile  
APP

## LAYERS OF APPLICATION

**MY COMPANIES**Cadastral  
Platform**SCDE**

Measurements

**SIGA**Asset  
Management**AUCTIONS**Energy  
Auctions**MVE**Sale of  
Surpluses**EXPORT**Energy  
Export**CLIQCEE**Online  
Modules**CLIQCEE**Calculation  
Engine**DRI**Results and  
Information**SECTOR ACCOUNTS**Electric Sector  
Account  
Management**PENALTIES**Penalty  
Management**DISCONNECTION**Disconnection  
Management





The cultural imbalance between the sector's agents



Prioritizing the importance of cybersecurity



Legal penalties not established



The weaknesses of older measuring devices



The shortage of cybersecurity manpower



High investment values due to the appreciation of the Dollar



Difficulties in the delivery of equipment due to the shortage of electronic components



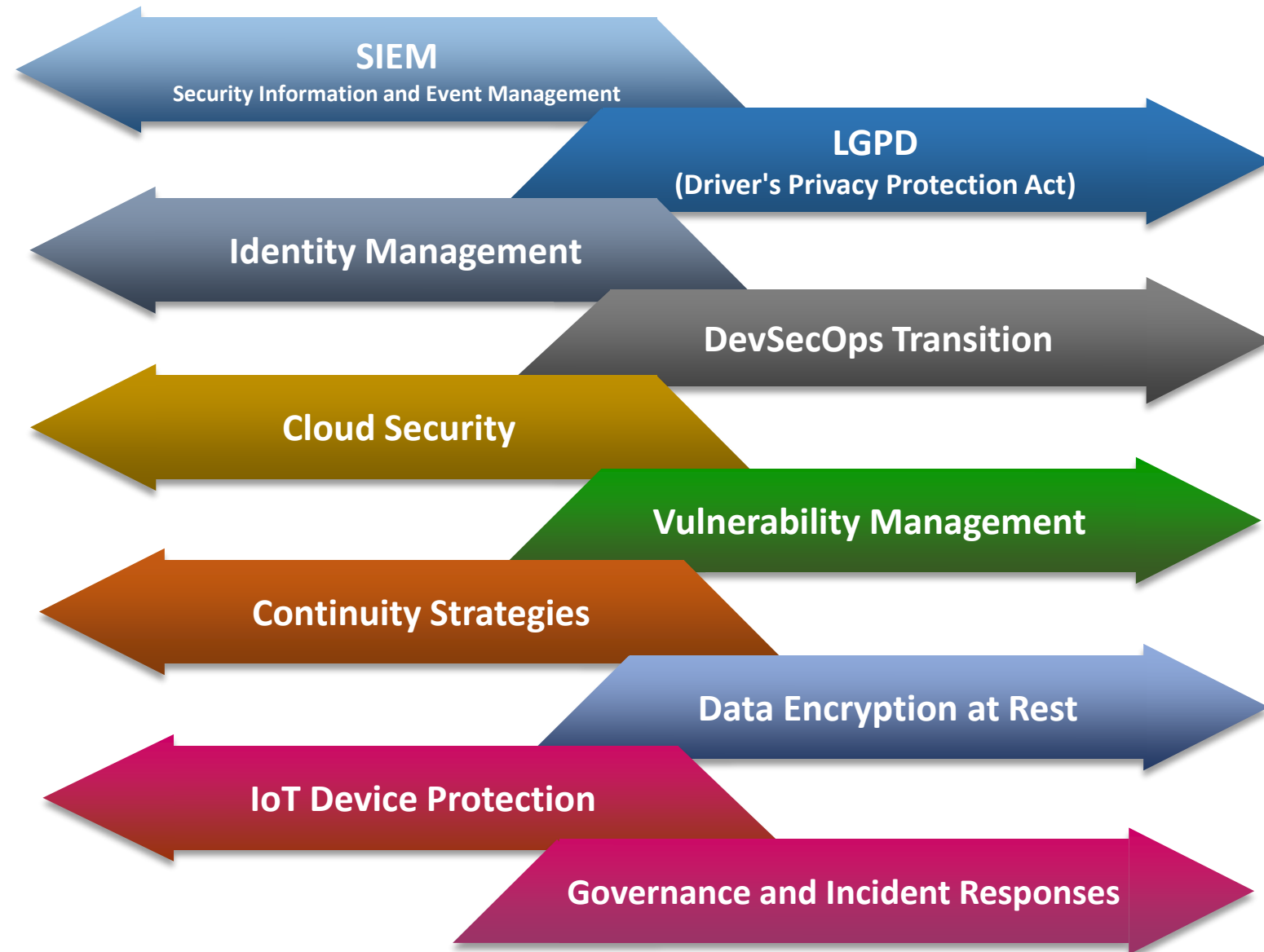
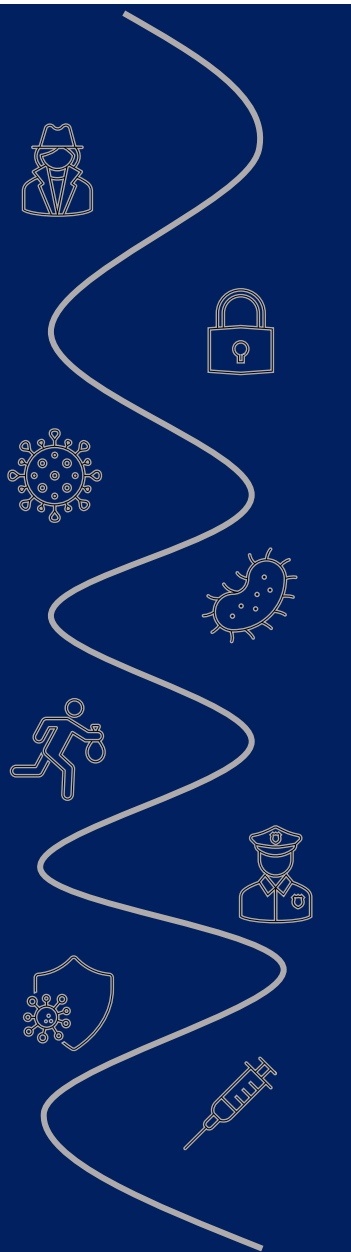
The entry of small consumer companies with little preparation for acting in cybersecurity



Cyber Threat Actors | Hacktivists | Organized Crime | “Insiders” and third parties









ccee

Câmara de Comercialização  
de Energia Elétrica

Thanks

